

Scorecard for

Fiserv

Generated February 1, 2019 by Dana Bowers (dana.bowers@venminder.com), Venminder

About this file

This file is a point-in-time capture of this Scorecard as of 2:14:15 PM EST, February 1, 2019. This file should not be confused for a pen test result or a final assessment.

Get the full picture with SecurityScorecard

SecurityScorecard offers ongoing self-monitoring, history reports, CSV data exports, and more to help security teams protect their organizations. For full free access to your organization's Scorecard, create an account today at bit.ly/2P8okyb.

Learn more about SecurityScorecard at bit.ly/2xXNg4N today.

What is SecurityScorecard?

SecurityScorecard is a security ratings service that uses an easy-to-understand A-F grading system to rate companies on their overall security as well as across 10 major risk factors. A company with a C, D, or F rating is 5.4 times more likely to suffer a consequential breach versus A or B-rated companies¹. Certain risk factors, such as application security and patching cadence, are even more indicative of the likelihood of breach. An F versus an A in these factors may translate into a tenfold increase in the likelihood of a data breach or successful attack.

Learn more about SecurityScorecard's rating system at bit.ly/2zMLSmW.

¹New SecurityScorecard Research Can Help You Detect a Data Breach Before It Happens', bit.ly/2yc0JVN

Next Steps: Get to an A



1. Create an account

This file has a lot of detail but remember, it's only for one point in time. Create an account to get full free access to your organizaton's Scorecard along with ongoing self-monitoring, history reports, CSV data exports and more.

2. Validate your Digital Footprint

Once you have an account, review your company's Digital Footprint, the assets SecurityScorecard found as potentially attributable to your company that affect the ratings in your Scorecard. Request removal or addition of IPs as needed.

3. Review issue findings

Investigate the contents of your Scorecard with your team(s). It's a win for your company's security posture when you identify loose ends of which you weren't aware.

4. Remediate issues, improve your score

Whether you've deployed a fix, found assets that don't belong to your company, or want to share information about compensating controls, you can let us know by remediating the identified finding(s) and submitting them for resolution approval. Resolutions are handled by our Support team, which will resolve any outstanding item within three business days. Remediate issues within the platform or email support@securityscorecard.io.

We're here to help

The SecurityScorecard platform is based on transparency and collaboration. Our Customer Reliability Support team provides remediation and resolution services at no charge and are happy to work with you and your customers to resolve any issues. If you need assistance at any stage, get in touch by emailing support@securityscorecard.io.

Scorecard Overview



Fiserv

76 Security Score

DOMAIN: fiserv.com

INDUSTRY: INFORMATION

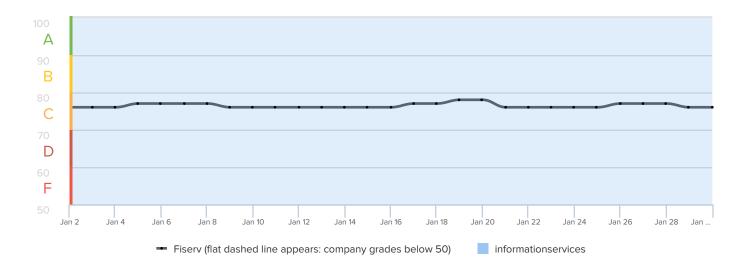
SERVICES

Factors

© 73 NETWORK SECURITY	20 ISSUES	F 58 APPLICATION SECURITY	13 ISSUES
F 51 DNS HEALTH	3 ISSUES	© 70 CUBIT SCORE	1 ISSUE
© 76 PATCHING CADENCE	6 ISSUES	A 100 HACKER CHATTER	0 ISSUES
B 89 ENDPOINT SECURITY	1 ISSUE	(A) 100 INFORMATION LEAK	0 ISSUES
A 100 IP REPUTATION	1 ISSUE	A 100 SOCIAL ENGINEERING	1 ISSUE

30-Day Score History

The chart below shows the evolution of the company's relative security ranking over time. The shaded area represents the range of values taken by companies in the INFORMATION SERVICES industry.



Peaks in score performance represent improvements to overall security posture, remediation of open issues, and improved efforts to protect company infrastructure. Dips reflect introduction of system and application misconfigurations, prolonged malware activity.

Action Items

FACTOR	SEVERITY	SCORE IMPACT	ISSUES DETECTED
IP Reputation	0	N/A	Malware Events, Last Year. Communications indicative of malware infections were observed over the last 365 days.
Endpoint Security	•	-0.4	Outdated Web Browser Observed. An outdated web browser connected to a web server.
Patching Cadence	•	-0.4	High-Severity Vulnerability in Last Observation. We observed a high-severity vulnerability during our last scan, which may still be publicly exposed.
	•	-0.9	High Severity CVEs Patching Cadence. High severity vulnerability seen on network more than 30 days after CVE was published.
	•	-0.4	End-of-Life Product. We observed an end-of-life product, one that is no longer developed or sold, publicly exposed.
	•	-0.6	Medium-Severity Vulnerability in Last Observation. We observed a medium- severity vulnerability during our last scan, which may still be publicly exposed.
	•	-0.7	Medium Severity CVEs Patching Cadence. Medium severity vulnerability seen on network more than 60 days after CVE was published.
	•	-0.1	End-of-Service Product. We observed an end-of-service product, one that is no longer supported by the manufacturer, publicly exposed.
Network Security	•	-0.5	SSH Software Supports Vulnerable Protocol. Server(s) observed running SSH software that support an SSH protocol lower than version 2.
	(1)	-0.2	MySQL Service Observed. We observed MySQL, a database management system, publicly exposed.
	(1)	-0.7	SSL Certificate Uses Weak Signature. TLS analysis reveals a weak signature algorithms, using SHA1 or MD5.
	(1)	-0.3	SSH Supports Weak MAC. A weak Message Authentication Code (MAC) algorithm has been detected.
	•	-0.3	SSH Supports Weak Cipher. A weak cipher has been detected.
	(1)	-0.1	Microsoft SQL Server Service Observed. We observed Microsoft SQL Server, a database management system, publicly exposed.
	•	-0.2	Certificate Is Self-Signed. Servers presenting self-signed certificates trigger warnings in, or prevent connections from TLS clients.
	•	-0.6	Certificate Is Expired. Expired certificates prevent TLS clients from connecting to servers.
	•	-<0.1	IMAP Service Observed. We observed IMAP, an email retrieval service, publicly exposed.
	•	-0.1	RDP Service Observed. We observed RDP, a remote access service, publicly exposed.
	•	-0.5	TLS Protocol Uses Weak Cipher. TLS analysis reveals a weak cipher either through encryption protocol or public key length.

•

-0.2

SMB Service Observed. We observed SMB, a file and printer-sharing service, publicly exposed.

FACTOR	SEVERITY	SCORE IMPACT	ISSUES DETECTED
Network Security	0	-<0.1	TLS Certificate Without Revocation Control. We observed a TLS certificate that did not contain either CRL or OCSP URLs.
	1	-0.1	FTP Service Observed. We observed FTP, a file-sharing service, publicly exposed.
		-<0.1	Telnet Service Observed. We observed Telnet, a remote access service, publicly exposed.
	1	-0.1	Certificate Lifetime Is Longer Than Best Practices. We observed a certificate with a lifetime longer than 39 Months.
Cubit Score	0	-1.0	Exposed Subdomain. An administrative subdomain was detected on public Internet. That subdomain may be vulnerable to unauthorized access.
Application Security	•	-1.6	Site does not enforce HTTPS. Site does not enforce the use of HTTPS encryption, leaving the user vulnerable to man-in-the-middle attackers (who can falsify data and inject malicious code).
	•	-0.9	Website does not implement X-Frame-Options Best Practices. Not explicitly setting X-Frame-Options allows other, untrusted, websites to embed your site in a frame on their page. This can be used to make social engineering attacks appear more legitimate, or can even be used for clickjacking attacks.
	•	-1.0	Website Does Not Implement HSTS Best Practices. Even if a website is protected with HTTPS, most browsers will still try first to connect to the HTTP version of the website unless explicitly specified. At that moment, visitors to the website are vulnerable to a man-in-the-middle attacker that can prevent them from reaching the HTTPS version of the website they intended to visit and instead divert them to a malicious website. The (expand) HSTS header ensures that, after a user's initial visit to the website, that they will not be susceptible to this man-in-the-middle attack because they will immediately connect to the HTTPS-protected website.
	•	-0.9	Website does not implement X-XSS-Protection Best Practices. Not explicitly setting X-XSS-Protection means that clients viewing a website could be at risk of reflected Cross-site Scripting (XSS) attacks.
	•	-0.9	Redirect Chain Contains HTTP. Site redirects through URLs that are not secured with HTTPS; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the intended destination site.
	•	-0.9	Insecure HTTPS Redirect Pattern. Site redirects to a domain in a way that limits the security provided by HTTPS and HTTP Strict Transport Security (HSTS) headers; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the site.
	•	-0.2	Session Cookie Missing 'HttpOnly' Attribute. Data may be exposed to unauthorized parties during cookie transmission and increases the risk of cross-site scripting (XSS) attacks.
		-0.3	Website does not implement X-Content-Type-Options Best Practices. Browsers will sometimes analyze the content themselves and handle it counter to the MIME type header; this can lead to security issues and execution of malicious code. For example, an attacker could hide malicious code with an image extension, where the browser does introspection and executes it as JavaScript.
DNIC IIIIII-		24	On a DNC Database Database Mining Committee DNC and a second database datab

DNS Health	₩	-2.1	Upen DNS Resolver Detected. Misconfigured DNS services were detected.
	•	-4.3	SPF Record Missing. A missing SPF record has been detected for a domain.
	•	-1.6	SPF Record Contains a Softfail. Softfail attributes in SPF makes spoofing and phishing email possible.



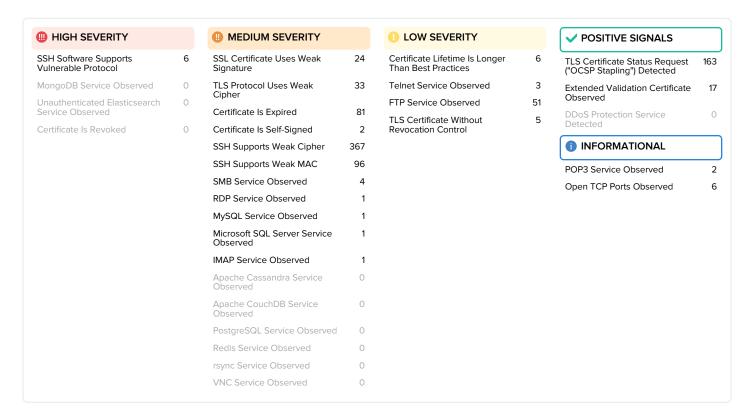
NETWORK SECURITY

ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

The Network Security module checks public datasets for evidence of high risk or insecure open ports within the company network. Insecure ports can often be exploited to allow an attacker to circumvent the login process or obtain elevated access to the system. If misconfigured, the open port can act as the entry point between a hacker's workstation and your internal network.



NETWORK SECURITY > ISSUE DETAIL

SSH Software Supports Vulnerable Protocol

Server(s) observed running SSH software that support an SSH protocol lower than version 2.

-0.5 SCORE

6 findings

EVIDENCE	DESTINATION IP	DESTINATION PORT	LAST SEEN
protocol 1.99	12.111.185.3	22	2019-01-09T18:35:31.265Z
protocol 1.99	8.18.18.224	22	2019-01-09T15:40:05.164Z
protocol 1.99	12.34.24.25	22	2019-01-09T14:54:13.389Z
protocol 1.99	12.111.185.1	22	2019-01-09T09:03:31.584Z
	protocol 1.99 protocol 1.99 protocol 1.99	protocol 1.99 12.111.185.3 protocol 1.99 8.18.18.224 protocol 1.99 12.34.24.25	protocol 1.99 12.111.185.3 22 protocol 1.99 8.18.18.224 22 protocol 1.99 12.34.24.25 22

SSH-1.99-Cisco-1.25\n	protocol 1.99	8.18.18.242	22	2019-01-09T07:25:19.459Z
-	protocol 1.99	12.111.185.2	22	2019-01-08T02:27:03.000Z

RECOMMENDATION

Configure the SSH service to support only SSH protocol version 2 or higher. Upgrade the SSH service software to the latest version of software.

ABOUT THIS ISSUE

Secure Shell (SSH) is an encrypted network protocol to allow remote login and other network services to operate securely over an unsecured network by providing an authenticated and encrypted channel. All modern SSH clients and servers support the more secure SSH protocol version 2, and any version older is exploitable and obsolete. Version 1 of the SSH protocol contains fundamental weaknesses including a design flaw that allows a man-in-the-middle attack. Findings are removed automatically if they have not been observed for more than 30 days.

NETWORK SECURITY > ISSUE DETAIL

SSH Supports Weak Cipher

A weak cipher has been detected.

367 findings

-0.3 SCORE

BANNER	EVIDENCE	DESTINATION IP	DESTINATION PORT	LAST SEEN
SSH-2.0-Serv-U_15.1.4.6	rijndael-cbc@lysator.liu.se	12.175.11.84	22	2019-01-09T21:06:31.168Z
SSH-2.0-Serv-U_15.1.4.6	blowfish-cbc	12.175.11.84	22	2019-01-09T21:06:31.168Z
SSH-2.0-Serv-U_15.1.4.6	rijndael256-cbc	12.175.11.84	22	2019-01-09T21:06:31.168Z
SSH-2.0-Serv-U_15.1.4.6	aes192-cbc	12.175.11.84	22	2019-01-09T21:06:31.168Z
SSH-2.0-Serv-U_15.1.4.6	cast128-cbc	12.175.11.84	22	2019-01-09T21:06:31.168Z
SSH-2.0-Serv-U_15.1.4.6	aes256-cbc	12.175.11.84	22	2019-01-09T21:06:31.168Z
SSH-2.0-Serv-U_15.1.4.6	rijndael192-cbc	12.175.11.84	22	2019-01-09T21:06:31.168Z
SSH-2.0-9.99	cast128-cbc	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	3des-cbc	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	twofish-cbc	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	aes128-cbc	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	twofish128-cbc	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	blowfish-cbc	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	twofish256-cbc	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	aes256-cbc	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	arcfour	63.167.86.240	22	2019-01-09T20:44:40.680Z

SSH-2.0-9.99	blowfish-cbc	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	aes128-cbc	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	cast128-cbc	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	twofish-cbc	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	arcfour	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	aes256-cbc	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	3des-cbc	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	twofish256-cbc	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	twofish128-cbc	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	twofish-cbc	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	blowfish-cbc	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	aes128-cbc	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	cast128-cbc	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	twofish256-cbc	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	arcfour	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	3des-cbc	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	twofish128-cbc	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	aes256-cbc	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	twofish-cbc	192.131.55.3	22	2019-01-09T20:02:54.001Z
SSH-2.0-9.99	aes128-cbc	192.131.55.3	22	2019-01-09T20:02:54.001Z
SSH-2.0-9.99	twofish256-cbc	192.131.55.3	22	2019-01-09T20:02:54.001Z
SSH-2.0-9.99	aes256-cbc	192.131.55.3	22	2019-01-09T20:02:54.001Z
SSH-2.0-9.99	twofish128-cbc	192.131.55.3	22	2019-01-09T20:02:54.001Z
SSH-2.0-OBS	arcfour128	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	aes192-cbc	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	aes256-cbc	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	aes128-cbc	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	3des-cbc	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	arcfour256	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	aes256-cbc	198.167.0.223	22	2019-01-09T19:46:51.225Z
SSH-2.0-OBS	arcfour128	198.167.0.223	22	2019-01-09T19:46:51.225Z

SSH-2.0-OBS	3des-cbc	198.167.0.223	22	2019-01-09T19:46:51.225Z
SSH-2.0-OBS	aes192-cbc	198.167.0.223	22	2019-01-09T19:46:51.225Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.223	22	2019-01-09T19:46:51.225Z
SSH-2.0-OBS	arcfour256	198.167.0.223	22	2019-01-09T19:46:51.225Z
SSH-2.0-OBS	aes128-cbc	198.167.0.223	22	2019-01-09T19:46:51.225Z
SSH-2.0-1.82_sshlib	3des-cbc	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	blowfish-cbc	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	aes128-cbc	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	twofish-cbc	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	aes256-cbc	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	twofish256-cbc	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	cast128-cbc	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	arcfour	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	twofish128-cbc	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-OBS	aes128-cbc	198.167.0.10	22	2019-01-09T19:37:04.641Z
SSH-2.0-OBS	aes256-cbc	198.167.0.10	22	2019-01-09T19:37:04.641Z
SSH-2.0-OBS	3des-cbc	198.167.0.10	22	2019-01-09T19:37:04.641Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.10	22	2019-01-09T19:37:04.641Z
SSH-2.0-OBS	aes192-cbc	198.167.0.10	22	2019-01-09T19:37:04.641Z
SSH-2.0- VShell_4_2_3_1188	twofish-cbc	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0- VShell_4_2_3_1188	3des-cbc	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0- VShell_4_2_3_1188	aes256-cbc	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0- VShell_4_2_3_1188	blowfish-cbc	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0- VShell_4_2_3_1188	aes192-cbc	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0- VShell_4_2_3_1188	aes128-cbc	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0- VShell_4_2_3_1188	arcfour	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0-OBS	arcfour256	198.167.0.64	22	2019-01-09T18:53:53.441Z
SSH-2.0-OBS	3des-cbc	198.167.0.64	22	2019-01-09T18:53:53.441Z

SSH-2.0-OBS	blowfish-cbc	198.167.0.64	22	2019-01-09T18:53:53.441Z
SSH-2.0-OBS	aes128-cbc	198.167.0.64	22	2019-01-09T18:53:53.441Z
SSH-2.0-OBS	aes192-cbc	198.167.0.64	22	2019-01-09T18:53:53.441Z
SSH-2.0-OBS	aes256-cbc	198.167.0.64	22	2019-01-09T18:53:53.441Z
SSH-2.0-OBS	arcfour128	198.167.0.64	22	2019-01-09T18:53:53.441Z
SSH-2.0-OpenSSH_5.4p1	aes256-cbc	65.206.30.70	22	2019-01-09T18:52:23.505Z
SSH-2.0-OpenSSH_5.4p1	aes128-cbc	65.206.30.70	22	2019-01-09T18:52:23.505Z
SSH-2.0-OpenSSH_5.4p1	arcfour	65.206.30.70	22	2019-01-09T18:52:23.505Z
SSH-2.0-OpenSSH_5.4p1	arcfour256	65.206.30.70	22	2019-01-09T18:52:23.505Z
SSH-2.0-9.99	twofish128-cbc	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	aes256-cbc	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	twofish-cbc	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	3des-cbc	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	cast128-cbc	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	blowfish-cbc	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	arcfour	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	aes128-cbc	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	twofish256-cbc	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-OBS	arcfour256	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	aes128-cbc	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	3des-cbc	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	aes192-cbc	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	aes256-cbc	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	arcfour128	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	arcfour256	198.167.0.172	22	2019-01-09T18:42:05.949Z
SSH-2.0-OBS	3des-cbc	198.167.0.172	22	2019-01-09T18:42:05.949Z
SSH-2.0-OBS	aes192-cbc	198.167.0.172	22	2019-01-09T18:42:05.949Z
SSH-2.0-OBS	aes128-cbc	198.167.0.172	22	2019-01-09T18:42:05.949Z
SSH-2.0-OBS	aes256-cbc	198.167.0.172	22	2019-01-09T18:42:05.949Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.172	22	2019-01-09T18:42:05.949Z
SSH-2.0-OBS	arcfour128	198.167.0.172	22	2019-01-09T18:42:05.949Z

SSH-1.99-Cisco-1.25	aes256-cbc	12.111.185.3	22	2019-01-09T18:35:31.137Z
SSH-1.99-Cisco-1.25	3des-cbc	12.111.185.3	22	2019-01-09T18:35:31.137Z
SSH-1.99-Cisco-1.25	aes192-cbc	12.111.185.3	22	2019-01-09T18:35:31.137Z
SSH-1.99-Cisco-1.25	aes128-cbc	12.111.185.3	22	2019-01-09T18:35:31.137Z
SSH-2.0-OBS	arcfour128	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	arcfour256	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	aes128-cbc	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	aes192-cbc	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	aes256-cbc	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	3des-cbc	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	3des-cbc	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-OBS	arcfour256	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-OBS	aes128-cbc	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-OBS	aes256-cbc	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-OBS	aes192-cbc	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-OBS	arcfour128	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-Cisco-1.25	aes192-cbc	65.202.81.137	22	2019-01-09T18:23:57.424Z
SSH-2.0-Cisco-1.25	aes128-cbc	65.202.81.137	22	2019-01-09T18:23:57.424Z
SSH-2.0-Cisco-1.25	aes256-cbc	65.202.81.137	22	2019-01-09T18:23:57.424Z
SSH-2.0-Cisco-1.25	3des-cbc	65.202.81.137	22	2019-01-09T18:23:57.424Z
SSH-2.0-9.99	twofish-cbc	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	arcfour	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	blowfish-cbc	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	cast128-cbc	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	twofish128-cbc	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	aes256-cbc	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	twofish256-cbc	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	3des-cbc	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	aes128-cbc	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-Cisco-1.25	aes192-cbc	12.2.10.241	22	2019-01-09T17:20:56.565Z

SSH-2.0-Cisco-1.25	3des-cbc	12.2.10.241	22	2019-01-09T17:20:56.565Z
SSH-2.0-Cisco-1.25	aes128-cbc	12.2.10.241	22	2019-01-09T17:20:56.565Z
SSH-2.0-Cisco-1.25	aes256-cbc	12.2.10.241	22	2019-01-09T17:20:56.565Z
SSH-2.0-OBS	aes128-cbc	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-OBS	arcfour128	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-OBS	aes192-cbc	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-OBS	arcfour256	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-OBS	3des-cbc	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-OBS	aes256-cbc	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-9.99	twofish128-cbc	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-9.99	aes128-cbc	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-9.99	cast128-cbc	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-9.99	twofish256-cbc	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-9.99	3des-cbc	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-9.99	aes256-cbc	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-9.99	twofish-cbc	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-9.99	arcfour	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-9.99	blowfish-cbc	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-1.82_sshlib	twofish256-cbc	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	cast128-cbc	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	aes256-cbc	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	aes128-cbc	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	arcfour	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	3des-cbc	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	twofish-cbc	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	twofish128-cbc	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	blowfish-cbc	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-9.99	aes128-cbc	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	arcfour	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	twofish-cbc	65.213.167.45	22	2019-01-09T15:10:18.326Z

SSH-2.0-9.99	twofish128-cbc	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	3des-cbc	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	blowfish-cbc	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	twofish256-cbc	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	cast128-cbc	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	aes256-cbc	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-1.99-Cisco-1.25	aes256-cbc	12.34.24.25	22	2019-01-09T14:54:14.588Z
SSH-1.99-Cisco-1.25	aes128-cbc	12.34.24.25	22	2019-01-09T14:54:14.588Z
SSH-1.99-Cisco-1.25	aes192-cbc	12.34.24.25	22	2019-01-09T14:54:14.588Z
SSH-1.99-Cisco-1.25	3des-cbc	12.34.24.25	22	2019-01-09T14:54:14.588Z
SSH-2.0-OBS	aes256-cbc	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-OBS	arcfour256	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-OBS	3des-cbc	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-OBS	aes192-cbc	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-OBS	aes128-cbc	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-OBS	arcfour128	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-9.99	aes256-cbc	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	blowfish-cbc	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	arcfour	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	cast128-cbc	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	twofish128-cbc	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	aes128-cbc	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	3des-cbc	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	twofish256-cbc	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	twofish-cbc	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-OBS	arcfour128	198.167.0.70	22	2019-01-09T13:45:18.353Z
SSH-2.0-OBS	aes256-cbc	198.167.0.70	22	2019-01-09T13:45:18.353Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.70	22	2019-01-09T13:45:18.353Z
SSH-2.0-OBS	aes128-cbc	198.167.0.70	22	2019-01-09T13:45:18.353Z
SSH-2.0-OBS	arcfour256	198.167.0.70	22	2019-01-09T13:45:18.353Z
SSH-2.0-OBS	aes192-cbc	198.167.0.70	22	2019-01-09T13:45:18.353Z

SSH-2.0-OBS	3des-cbc	198.167.0.70	22	2019-01-09T13:45:18.353Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	arcfour256	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	arcfour128	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	aes128-cbc	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	aes256-cbc	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	aes192-cbc	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	3des-cbc	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	arcfour256	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	aes192-cbc	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	arcfour128	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	aes128-cbc	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	aes256-cbc	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	3des-cbc	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	aes256-cbc	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-OBS	3des-cbc	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-OBS	arcfour256	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-OBS	aes192-cbc	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-OBS	aes128-cbc	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-OBS	arcfour128	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-9.99	aes128-cbc	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	twofish256-cbc	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	3des-cbc	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	cast128-cbc	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	twofish-cbc	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	aes256-cbc	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	blowfish-cbc	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	twofish128-cbc	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	arcfour	65.213.167.80	22	2019-01-09T12:41:55.960Z

SSH-2.0-OBS	aes192-cbc	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-OBS	aes128-cbc	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-OBS	3des-cbc	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-OBS	aes256-cbc	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-OBS	arcfour256	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-OBS	arcfour128	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-mod_sftp/0.9.9	arcfour128	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-mod_sftp/0.9.9	aes256-cbc	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-mod_sftp/0.9.9	3des-cbc	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-mod_sftp/0.9.9	blowfish-cbc	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-mod_sftp/0.9.9	arcfour256	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-mod_sftp/0.9.9	aes192-cbc	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-mod_sftp/0.9.9	cast128-cbc	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-mod_sftp/0.9.9	aes128-cbc	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-9.99	twofish-cbc	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	3des-cbc	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	twofish256-cbc	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	blowfish-cbc	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	aes128-cbc	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	cast128-cbc	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	twofish128-cbc	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	aes256-cbc	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	blowfish-cbc	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0-9.99	aes256-cbc	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0-9.99	twofish128-cbc	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0-9.99	twofish-cbc	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0-9.99	cast128-cbc	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0-9.99	arcfour	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0-9.99	twofish256-cbc	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0-9.99	3des-cbc	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0-9.99	aes128-cbc	63.167.86.246	22	2019-01-09T11:35:22.579Z

SSH-2.0- dropbear_2014.65	twofish-cbc	65.206.30.72	22	2019-01-09T11:33:22.217Z
SSH-2.0- dropbear_2014.65	twofish128-cbc	65.206.30.72	22	2019-01-09T11:33:22.217Z
SSH-2.0- dropbear_2014.65	aes128-cbc	65.206.30.72	22	2019-01-09T11:33:22.217Z
SSH-2.0- dropbear_2014.65	aes256-cbc	65.206.30.72	22	2019-01-09T11:33:22.217Z
SSH-2.0- dropbear_2014.65	3des-cbc	65.206.30.72	22	2019-01-09T11:33:22.217Z
SSH-2.0- dropbear_2014.65	twofish256-cbc	65.206.30.72	22	2019-01-09T11:33:22.217Z
SSH-2.0- VShell_3_6_6_741	aes256-cbc	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0- VShell_3_6_6_741	arcfour	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0- VShell_3_6_6_741	aes192-cbc	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0- VShell_3_6_6_741	3des-cbc	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0- VShell_3_6_6_741	blowfish-cbc	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0- VShell_3_6_6_741	twofish-cbc	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0- VShell_3_6_6_741	aes128-cbc	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0-OBS	arcfour128	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	arcfour256	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	aes256-cbc	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	aes192-cbc	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	aes128-cbc	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	3des-cbc	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	arcfour128	198.167.0.113	22	2019-01-09T10:58:56.163Z
SSH-2.0-OBS	3des-cbc	198.167.0.113	22	2019-01-09T10:58:56.163Z
SSH-2.0-OBS	aes128-cbc	198.167.0.113	22	2019-01-09T10:58:56.163Z
SSH-2.0-OBS	aes192-cbc	198.167.0.113	22	2019-01-09T10:58:56.163Z
SSH-2.0-OBS	aes256-cbc	198.167.0.113	22	2019-01-09T10:58:56.163Z

SSH-2.0-OBS	blowfish-cbc	198.167.0.113	22	2019-01-09T10:58:56.163Z
SSH-2.0-OBS	arcfour256	198.167.0.113	22	2019-01-09T10:58:56.163Z
SSH-2.0-9.99	twofish128-cbc	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	aes256-cbc	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	blowfish-cbc	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	cast128-cbc	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	arcfour	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	twofish256-cbc	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	3des-cbc	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	twofish-cbc	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	aes128-cbc	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-OBS	arcfour128	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-OBS	aes192-cbc	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-OBS	aes256-cbc	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-OBS	3des-cbc	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-OBS	arcfour256	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-OBS	aes128-cbc	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-5.37	3des-cbc	198.246.218.142	22	2019-01-09T09:22:42.918Z
SSH-2.0-5.37	aes256-cbc	198.246.218.142	22	2019-01-09T09:22:42.918Z
SSH-2.0-9.99	aes128-cbc	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	twofish-cbc	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	arcfour	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	twofish256-cbc	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	twofish128-cbc	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	aes256-cbc	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	cast128-cbc	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	3des-cbc	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	blowfish-cbc	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-OBS	3des-cbc	198.167.0.180	22	2019-01-09T09:10:22.455Z
SSH-2.0-OBS	aes256-cbc	198.167.0.180	22	2019-01-09T09:10:22.455Z
SSH-2.0-OBS	aes128-cbc	198.167.0.180	22	2019-01-09T09:10:22.455Z

SSH-2.0-OBS	arcfour128	198.167.0.180	22	2019-01-09T09:10:22.455Z
SSH-2.0-OBS	arcfour256	198.167.0.180	22	2019-01-09T09:10:22.455Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.180	22	2019-01-09T09:10:22.455Z
SSH-2.0-OBS	aes192-cbc	198.167.0.180	22	2019-01-09T09:10:22.455Z
SSH-2.0-9.99	cast128-cbc	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	arcfour	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	aes128-cbc	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	aes256-cbc	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	twofish128-cbc	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	3des-cbc	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	blowfish-cbc	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	twofish-cbc	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	twofish256-cbc	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	3des-cbc	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	twofish-cbc	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	aes128-cbc	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	arcfour	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	twofish256-cbc	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	cast128-cbc	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	twofish128-cbc	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	aes256-cbc	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	blowfish-cbc	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-1.99-Cisco-1.25	aes192-cbc	12.111.185.1	22	2019-01-09T09:03:31.581Z
SSH-1.99-Cisco-1.25	3des-cbc	12.111.185.1	22	2019-01-09T09:03:31.581Z
SSH-1.99-Cisco-1.25	aes256-cbc	12.111.185.1	22	2019-01-09T09:03:31.581Z
SSH-1.99-Cisco-1.25	aes128-cbc	12.111.185.1	22	2019-01-09T09:03:31.581Z
SSH-2.0-9.99	aes256-cbc	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	arcfour	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	twofish-cbc	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	3des-cbc	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	twofish128-cbc	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	aes128-cbc	63.84.245.78	22	2019-01-09T08:05:53.337Z

SSH-2.0-9.99	cast128-cbc	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	twofish256-cbc	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	blowfish-cbc	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-OBS	arcfour256	198.167.0.142	22	2019-01-09T07:46:04.881Z
SSH-2.0-OBS	arcfour128	198.167.0.142	22	2019-01-09T07:46:04.881Z
SSH-2.0- VShell_3_8_2_229	aes128-cbc	65.118.57.177	22	2019-01-09T07:29:18.485Z
SSH-2.0- VShell_3_8_2_229	aes256-cbc	65.118.57.177	22	2019-01-09T07:29:18.485Z
SSH-2.0- VShell_3_8_2_229	arcfour	65.118.57.177	22	2019-01-09T07:29:18.485Z
SSH-2.0- VShell_3_8_2_229	blowfish-cbc	65.118.57.177	22	2019-01-09T07:29:18.485Z
SSH-2.0- VShell_3_8_2_229	3des-cbc	65.118.57.177	22	2019-01-09T07:29:18.485Z
SSH-2.0- VShell_3_8_2_229	aes192-cbc	65.118.57.177	22	2019-01-09T07:29:18.485Z
SSH-2.0- VShell_3_8_2_229	twofish-cbc	65.118.57.177	22	2019-01-09T07:29:18.485Z

RECOMMENDATION

Configure the SSH server to disable Arcfour and CBC ciphers.

ABOUT THIS ISSUE

The SSH server is configured to support either Arcfour or Cipher Block Chaining (CBC) mode cipher algorithms. SSH can be configured to use Counter (CTR) mode encryption instead of CBC. The use of Arcfour algorithms should be disabled.

NETWORK SECURITY > ISSUE DETAIL

SSH Supports Weak MAC

A weak Message Authentication Code (MAC) algorithm has been detected.

-0.3 SCORE

96 findings

BANNER	EVIDENCE	DESTINATION IP	DESTINATION PORT	LAST SEEN
SSH-2.0-9.99	hmac-md5-96	208.66.22.159	22	2019-01-09T21:00:22.868Z
SSH-2.0-9.99	hmac-md5	208.66.22.159	22	2019-01-09T21:00:22.868Z
SSH-2.0-9.99	hmac-md5-96	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	hmac-md5	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	hmac-md5	209.163.213.146	22	2019-01-09T20:30:04.493Z

		000 400 040 440	00	
SSH-2.0-9.99	hmac-md5-96	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	hmac-md5	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	hmac-md5-96	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	hmac-md5	208.66.22.64	22	2019-01-09T20:01:46.446Z
SSH-2.0-9.99	hmac-md5-96	208.66.22.64	22	2019-01-09T20:01:46.446Z
SSH-2.0-OBS	hmac-md5	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.223	22	2019-01-09T19:46:51.225Z
SSH-2.0-OBS	hmac-md5	198.167.0.223	22	2019-01-09T19:46:51.225Z
SSH-2.0-1.82_sshlib	hmac-md5-96	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	hmac-md5	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-OBS	hmac-md5	198.167.0.10	22	2019-01-09T19:37:04.641Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.10	22	2019-01-09T19:37:04.641Z
SSH-2.0- VShell_4_2_3_1188	hmac-md5	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0- VShell_4_2_3_1188	hmac-md5-96	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.64	22	2019-01-09T18:53:53.441Z
SSH-2.0-OBS	hmac-md5	198.167.0.64	22	2019-01-09T18:53:53.441Z
SSH-2.0-OpenSSH_5.4p1	hmac-md5-96	65.206.30.70	22	2019-01-09T18:52:23.505Z
SSH-2.0-OpenSSH_5.4p1	hmac-md5	65.206.30.70	22	2019-01-09T18:52:23.505Z
SSH-2.0-9.99	hmac-md5-96	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	hmac-md5	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-OBS	hmac-md5	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.172	22	2019-01-09T18:42:05.949Z
SSH-2.0-OBS	hmac-md5	198.167.0.172	22	2019-01-09T18:42:05.949Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	hmac-md5	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	hmac-md5	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-9.99	hmac-md5	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	hmac-md5-96	12.168.16.253	22	2019-01-09T18:16:32.721Z

SSH-2.0-OBS	hmac-md5-96	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-OBS	hmac-md5	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-9.99	hmac-md5-96	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-1.82_sshlib	hmac-md5-96	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	hmac-md5	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-9.99	hmac-md5-96	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	hmac-md5	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	hmac-md5	208.66.22.71	22	2019-01-09T15:04:27.380Z
SSH-2.0-9.99	hmac-md5-96	208.66.22.71	22	2019-01-09T15:04:27.380Z
SSH-2.0-OBS	hmac-md5	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-9.99	hmac-md5	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	hmac-md5-96	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.70	22	2019-01-09T13:45:18.353Z
SSH-2.0-OBS	hmac-md5	198.167.0.70	22	2019-01-09T13:45:18.353Z
SSH-2.0-OBS	hmac-md5	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	hmac-md5	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-OBS	hmac-md5	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-9.99	hmac-md5	208.66.22.12	22	2019-01-09T12:50:38.795Z
SSH-2.0-9.99	hmac-md5-96	208.66.22.12	22	2019-01-09T12:50:38.795Z
SSH-2.0-9.99	hmac-md5-96	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	hmac-md5	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-OBS	hmac-md5	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-mod_sftp/0.9.9	hmac-md5-96	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-mod_sftp/0.9.9	hmac-md5	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-9.99	hmac-md5-96	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	hmac-md5	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	hmac-md5	63.167.86.246	22	2019-01-09T11:35:22.579Z

SSH-2.0-9.99	hmac-md5-96	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0- dropbear_2014.65	hmac-md5	65.206.30.72	22	2019-01-09T11:33:22.217Z
SSH-2.0- VShell_3_6_6_741	hmac-md5	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0- VShell_3_6_6_741	hmac-md5-96	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0-OBS	hmac-md5	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.113	22	2019-01-09T10:58:56.163Z
SSH-2.0-OBS	hmac-md5	198.167.0.113	22	2019-01-09T10:58:56.163Z
SSH-2.0-9.99	hmac-md5-96	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	hmac-md5	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-OBS	hmac-md5	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-9.99	hmac-md5	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	hmac-md5-96	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-OBS	hmac-md5	198.167.0.180	22	2019-01-09T09:10:22.455Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.180	22	2019-01-09T09:10:22.455Z
SSH-2.0-9.99	hmac-md5	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	hmac-md5-96	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	hmac-md5-96	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	hmac-md5	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	hmac-md5-96	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	hmac-md5	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	hmac-md5-96	208.66.22.35	22	2019-01-09T07:50:09.004Z
SSH-2.0-9.99	hmac-md5	208.66.22.35	22	2019-01-09T07:50:09.004Z
SSH-2.0-9.99	hmac-md5-96	12.168.17.253	22	2019-01-09T07:34:44.151Z
SSH-2.0-9.99	hmac-md5	12.168.17.253	22	2019-01-09T07:34:44.151Z
SSH-2.0- VShell_3_8_2_229	hmac-md5	65.118.57.177	22	2019-01-09T07:29:18.485Z
SSH-2.0- VShell_3_8_2_229	hmac-md5-96	65.118.57.177	22	2019-01-09T07:29:18.485Z

RECOMMENDATION

Configure the SSH server to disable the use of MD5.

ABOUT THIS ISSUE

The SSH server is configured to support MD5 algorithm. The cryptographic strength depends upon the size of the key and algorithm that is used. A Modern MAC algorithms such as SHA1 or SHA2 should be used instead.

NETWORK SECURITY > ISSUE DETAIL

IMAP Service Observed

We observed IMAP, an email retrieval service, publicly exposed.

-<0.1 SCORE

1 finding

PRODUCT NAME	PRODUCT VERSION	DESTINATION IP	DESTINATION PORT	LAST SEEN	
Dovecot imapd	-	209.221.136.222	143	2018-12-30T14:58:32.606Z	
Banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready.\r\n					

RECOMMENDATION

Review the business necessity of hosting a public IMAP server, and remove it from the Internet if possible. If not possible, consider restricting the service by whitelisting the IP addresses that require access.

ABOUT THIS ISSUE

The IMAP protocol offers access to messages stored on email servers. IMAP servers frequently contain all messages ever sent or received by an email account, not just recent messages. We observed an IMAP service on the Internet, accessible by the public. Email retrieval services are attractive targets to attackers due to the data they may contain. An attacker that gains access to an email account's messages may use them for blackmail, impersonating the owner of the email account, or employ the information when launching further attacks. An attacker with access to an email account's messages may gain access to many online accounts associated with that email address by using the password reset functions available on most websites. Attackers may target the service with authentication bypass attacks (e.g., brute-forcing, buffer overflows, blank passwords) in an attempt to gain control of the host or access the messages within. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL

Microsoft SQL Server Service Observed

We observed Microsoft SQL Server, a database management system, publicly exposed.

-0.1 SCORE IMPACT

1 finding

PRODUCT NAME	PRODUCT VERSION	DESTINATION IP	DESTINATION PORT	LAST SEEN

Microsoft SQL Server 2014 12.00.2269 184.170.226.96 1433 2019-01-21T12:50:15.000Z

RECOMMENDATION

Exposing database services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by whitelisting the IP addresses that require access.

ABOUT THIS ISSUE

Microsoft SQL Server is a proprietary database management system (DBMS). DBMSes are intended to store large amounts of information. We observed a Microsoft SQL Server service on the Internet, accessible by the public. DBMSes are attractive targets to attackers due to the data they may contain. An attacker that breaches a DBMS may sell the databases within, use them for blackmail, or employ the information when launching further attacks. A breached database may result in legal proceedings, have public notification requirements, negatively impact public image, and have insurance implications. Attackers may target the service with authentication bypass attacks (e.g., bruteforcing, buffer overflows, blank passwords) in an attempt to gain control of the host or exfiltrate its databases. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL



We observed MySQL, a database management system, publicly exposed.

-0.2 SCORE

1 finding

PRODUCT NAME	PRODUCT VERSION	DESTINATION IP	DESTINATION PORT	LAST SEEN
MySQL	-	65.206.30.70	3306	2019-01-23T07:17:56.000Z

RECOMMENDATION

Exposing database services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by whitelisting the IP addresses that require access.

ABOUT THIS ISSUE

MySQL is an open-source database management system (DBMS). DBMSes are intended to store large amounts of information. We observed a MySQL service on the Internet, accessible by the public. DBMSes are attractive targets to attackers due to the data they may contain. An attacker that breaches a DBMS may sell the databases within, use them for blackmail, or employ the information when launching further attacks. A breached database may result in legal proceedings, have public notification requirements, negatively impact public image, and have insurance implications. Attackers may target the service with authentication bypass attacks (e.g., bruteforcing, buffer overflows, blank passwords) in an attempt to gain control of the host or exfiltrate its databases. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL

RDP Service Observed

We observed RDP, a remote access service, publicly exposed.

-0.1 SCORE IMPACT

1 finding

PRODUCT NAME	PRODUCT VERSION	DESTINATION IP	DESTINATION PORT	LAST SEEN
Microsoft Terminal Services	-	66.193.233.165	3389	2019-01-23T19:09:51.000Z

RECOMMENDATION

Exposing remote access services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by whitelisting the IP addresses that require access.

ABOUT THIS ISSUE

The RDP protocol offers remote access to a host, providing a view of the host's console as output and accepting keyboard and mouse events as input. We observed an RDP service on the Internet, accessible by the public. Remote access services are attractive targets to attackers because they provide remote control over a host. Once logged-in, users can install programs, access files, and run commands on the host. Attackers can add hosts over which they have gained control to botnets, adding the host's computational capabilities and bandwidth to their spam, malware, or distributed denial-of-service (DDoS) campaigns. Attackers may target the service with authentication bypass attacks (e.g., brute-forcing, buffer overflows, blank passwords) in an attempt to gain control of the host or exfiltrate its databases. Due to sharing user authentication databases with other Microsoft services, brute-forcing this service may provide credentials useful on other services. Attackers may launch denial-of-service (DoS) attacks against the service, rendering the service unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL

SMB Service Observed

We observed SMB, a file and printer-sharing service, publicly exposed.

-0.2 SCORE

4 findings

PRODUCT NAME	PRODUCT VERSION	DESTINATION IP	DESTINATION PORT	LAST SEEN
Microsoft Windows Server 2008 R2 - 2012 microsoft- ds	-	184.170.228.66	445	2019-01-18T10:49:38.000Z
Microsoft Windows netbios-ssn	-	184.170.228.66	139	2019-01-14T23:56:38.000Z

Microsoft Windows Server - 2008 R2 - 2012 microsoft-ds	184.170.225.205	445	2019-01-06T02:54:31.783Z
	x00\xfc\xe3\x01\x00\xfa\xa8\xfe\$k\xa5\xd4\x0	1,\x01\x08:\x00\xe4	0@\x06\x00\x00\x01\x00\x11\x07\x00\x032\x00\x01\ Y\x19\xac\xb4~J\xa7W\x00O\x00R\x00K\x00G\x00R\ 00\x00
Microsoft Windows - netbios-ssn	184.170.225.205	139	2019-01-03T06:40:56.600Z
Banner: \x83\x00\x00\x01\x8f			

RECOMMENDATION

Exposing SMB to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by whitelisting the IP addresses that require access.

ABOUT THIS ISSUE

The SMB protocol offers access to files, printers, and other services on a network. We observed an SMB service on the Internet, accessible by the public. These services are attractive targets to attackers due to the data they may contain, and the potential for access to other network resources. Attackers may target the service with authentication bypass attacks (e.g., bruteforcing, buffer overflows, blank passwords) in an attempt to gain control of the host or exfiltrate its databases. Due to sharing user authentication databases with other Microsoft services, bruteforcing this service may provide credentials useful on other services. Attackers may launch denial-of-service (DoS) attacks against the service, rendering the service unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL

Certificate Is Expired

Expired certificates prevent TLS clients from connecting to servers.

-0.6 SCORE

81 findings

SUBJECT COMMON NAME	ISSUER ORGANIZATION NAME	NOT VALID BEFORE	NOT VALID AFTER	DESTINATION IP	DESTINATION PORT
pacific- uat.hepsiian.com	GeoTrust, Inc.	2013-04- 15T16:10:14.000Z	2015-04- 18T17:11:51.000Z	64.149.172.189	443
morasp- btat1.fiservapps.com	GeoTrust Inc.	2017-01- 11T00:00:00.000Z	2019-01- 11T23:59:59.000Z	166.73.13.176	443
morasp- btat1.fiservapps.com	GeoTrust Inc.	2017-01- 11T00:00:00.000Z	2019-01- 11T23:59:59.000Z	166.73.13.179	443
mycheckfree- alpha.nc.checkfree.co m	GeoTrust Inc.	2016-02- 22T00:00:00.000Z	2018-02- 21T23:59:59.000Z	208.11.141.91	443
alpha- merchantselfcare.che ckfree.com	Equifax	2008-10- 17T14:35:55.000Z	2010-11- 17T15:35:55.000Z	208.11.141.178	443

www.fserv.com GeoTrust Inc. 2016-09-19170000000002 2018-09-29173 59-59-0002 2015-216-53.145 443 cert-ops.chck/decom GeoTrust, Inc. 2016-02-09170000000000 2018-02-2017-09-09173 59-59-0002 1981-246-154.178 443 **lending/fikerwaphs-com GeoTrust, Inc. 2018-09-000000000000000000000000000000000						
#senderifiere.com *Inding fiservepps.c om data delivery-ait- cert. onefiserv.com functifications functifications data delivery-ait- cert. onefiserv.com functifications functifications functifications functifications delib- serveri hepsilan.com delib- serveri hepsilan.com GeoTrust Inc. 2016-09- 13710-0000000000000000000000000000000000	www.fiserv.com	GeoTrust Inc.			205.216.53.145	443
Company Comp		GeoTrust Inc.			198.246.154.178	443
Connectdublin.checkfr GeoTrust, Inc. 2013-08- 2015-09- 2	-	GeoTrust, Inc.			198.246.154.33	443
di-lib					12.168.132.15	443
server.hepsilan.com 13100.00.00.000Z 13123.59:59.000Z achcpo-corput.liferervapps.com GeoTrust Inc. 2016-04-13100.000.000Z 12123.59:59.000Z 192.131.76.196 443 mcom-asp-bata onefiserv.com GeoTrust Inc. 2016-09-21700.000.000Z 2017-09-01723.59:59.000Z 192.131.76.225 443 "lending.fiservapps.com GeoTrust, Inc. 2013-09-04TH10.54.000Z 2017-09-06T05.06:26.000Z 192.131.76.78 443 mobilitiapps-bata onefiserv.com GeoTrust, Inc. 2016-09-2170.000Z 2018-09-2170.000Z 192.131.76.78 443 mcom-asp-bata onefiserv.com GeoTrust Inc. 2016-09-2170.000.000 2018-09-2170.000Z 192.131.76.62 443 av-billerdirectul-bata onefiserv.com Inc. 2016-09-2170.000.000 2018-09-2170.000 192.131.76.106 443 cardvallet-ws.fiservapps.com GeoTrust Inc. 2016-09-2170.000.0000 2018-09-21723.59:59.000Z 192.131.76.61 443 billierops-alpha.nc.checkfree.com GeoTrust, Inc. 2016-01-02-020.0000 2018-01-02-02-020.000 2018-01-02-02-020.0000 2018-01-02-02-020.0000 2011.141.77 443 alpha-apscheckfree.		GeoTrust, Inc.			12.16.164.14	443
uat.fiservapps.com 13T00.00.00.0000Z 13T23:59:59.000Z mcom-asp-blat-orefiserv.com GeoTrust Inc. 2016-09-21T23:59:59.000Z 192.131.76.59 443 ".lending.fiservapps.c om GeoTrust, Inc. 2013-09-2017-09-06T05:06:26.000Z 192.131.76.225 443 mobilitiapps-btat2.mybilis.com GeoTrust, Inc. 2014-04-28122:58:17.000Z 2016-05-30T16:58:17.000Z 192.131.76.78 443 mcom-asp-btat-orefiserv.com GeoTrust Inc. 2016-09-21700:00:00 2018-09-2172:359:59.000Z 192.131.76.106 443 mcom-asp-btat-orefiserv.com Trustwave Holdings, 2077-05-07706:07:54.000Z 2017-05-09-2172:05-000Z 192.131.76.106 443 mcom-asp-btat-orefiserv.com GeoTrust Inc. 2016-09-2170:00:00.0000Z 2018-09-2172:13-75-000Z 192.131.76.61 443 billerops-alpha.checkfree.com GeoTrust Inc. 2016-01-2017-21-20-2017-21-20-2017-21-20-2017-21-20-2017-21-20-2017-21-20-2017-21-20-2017-21-20-2017-21-20-2017-21-20-2017-21-20-20-2017-21-20-2017-21-20-20-20-20-20-20-20-20-20-20-20-20-20-		GeoTrust Inc.			64.149.172.214	443
btat.onefiserv.com *Iending.fiservapps.c om *Iending.fiservapps.c om		GeoTrust Inc.			192.131.76.196	443
om 04TH:10:54,000Z 06T05:06:26.000Z mobilitiapps-btat2.mybilis.com GeoTrust, Inc. 2014-04-28T22:58:17,000Z 2016-05-30T16:58:17.000Z 192.131.76.78 443 mcom-asp-btat.onefiserv.com GeoTrust Inc. 2016-09-21T00:00:00.0000Z 2018-09-21T23:59:59.000Z 192.131.76.106 443 mcom-asp-btat.onefiserv.com GeoTrust Inc. 2016-09-21T00:00:00.0000Z 2017-05-20T06:07:54.000Z 192.131.76.106 443 mcom-asp-btat.onefiserv.com GeoTrust Inc. 2016-09-21T00:00:00.0000Z 2018-09-21T23:59:59.000Z 192.131.76.61 443 cardvalet-ws.fiservapps.com GeoTrust Inc. 2016-01-01-03T00:00:00.000Z 2018-01-07723:59:59.000Z 50.58.9.223 443 billerops-sipha.nc.check/free.com GeoTrust Inc. 2012-02-2070:00:00:000Z 2014-02-21720:40:55.000Z 208.11.141.74 443 billerops-betan.check/free.com GeoTrust Inc. 2015-11-13700:00:00:00:00 2017-11-1272:59:59:000Z 208.11.141.77 443 beta-betan.check/free.com GeoTrust Inc. 2016-02-02-02700:00:00:000Z 2018-02-02-02700:000Z 208.11.141.177 443 bofa-alpha.nc.check/free.com GeoTru	·	GeoTrust Inc.			192.131.76.59	443
Data Lamphalist com Cardwalet common Cardwale	-	GeoTrust, Inc.			192.131.76.225	443
btat.onefiserv.com 21T00:00:00:00:00 21T23:59:59:00:00Z av-billerdirectui-btat.onefiserv.com Trustwave Holdings, Inc. 2015-05- 07T06:07:54.000Z 2017-05- 08T12:07:54.000Z 192:131.76:106 443 mcom-asp-btat.onefiserv.com GeoTrust Inc. 2016-09- 21T00:00:00.000Z 2018-09- 21T23:59:59.000Z 192:131.76:61 443 cardvalet-ws.fiservapps.com GeoTrust Inc. 2016-01- 2018-01- 08T00:00:00.000Z 50:58.9.223 443 billerops-alpha.nc.checkfree.com GeoTrust, Inc. 2012-02- 2014-02- 2014-02- 2014-02- 2014-02- 2014-02- 2014-02- 2014-02- 2014-02- 2014-02- 2014-04- 2014-0		GeoTrust, Inc.			192.131.76.78	443
btat.onefiserv.com Inc. 07T06:07:54.000Z 08T12:07:54.000Z mcom-asp- btat.onefiserv.com GeoTrust Inc. 2016-09- 21T00:00:00:000Z 2018-09- 21T23:59:59.000Z 192.131.76.61 443 cardvalet- ws.fiservapps.com GeoTrust Inc. 2016-01- 08T00:00:00:000Z 2018-01- 07T23:59:59.000Z 50.58.9.223 443 billerops- alpha- alpha- alpha- aps.checkfree.com GeoTrust, Inc. 2012-02- 20T07:32:54.000Z 2014-02- 21T20:40:55.000Z 208.11.141.74 443 billerops- beta- ps.checkfree.com GeoTrust, Inc. 2012-04- 08T20:46:41.000Z 2014-04- 12T04:43:20.000Z 208.11.141.77 443 sponsorcare- alpha.nc.checkfree.com GeoTrust Inc. 2016-02- 02T00:00:00.000Z 2018-02- 02T00:00:00.000Z 208.11.141.73 443 beta- yes.checkfree.com Equifax 2008-08- 19T15:22:11.000Z 2010-10- 19T15:22:11.000Z 208.11.141.177 443 bofa- alpha.nc.checkfree.co m GeoTrust Inc. 2016-02- 22T00:00:00.000Z 2018-02- 21T23:59:59.000Z 208.11.141.157 443	•	GeoTrust Inc.			192.131.76.62	443
btat.onefiserv.com 21T00:00:00.0000Z 21T23:59:59:000Z cardvalet-ws.fiservapps.com GeoTrust Inc. 2016-01-08T00:00:00.000Z 2018-01-07723:59:59:000Z 50.58.9.223 443 billerops-alpha.nc.checkfree.com GeoTrust, Inc. 2012-02-20T07:32:54:000Z 2014-02-21T20:40:55.000Z 208.11.141.74 443 alpha-aps.checkfree.com GeoTrust Inc. 2015-11-13T00:00:00.000Z 2017-11-12723:59:59.000Z 208.11.141.128 443 billerops-beta.nc.checkfree.com GeoTrust, Inc. 2012-04-2014-04-2014-04-08T20:46:41:000Z 2014-04-2000Z 208.11.141.77 443 sponsorcare-alpha.nc.checkfree.com GeoTrust Inc. 2016-02-2017-00:00:00:00:00:00:00:00:00:00:00:00:00:					192.131.76.106	443
ws.fiservapps.com 08T00:00:00:000Z 07T23:59:59:000Z billerops- alpha.nc.checkfree.co m GeoTrust, Inc. 2012-02- 20T07:32:54.000Z 2014-02- 21T20:40:55.000Z 208.11.141.74 443 alpha- aps.checkfree.com GeoTrust Inc. 2015-11- 13T00:00:00.000Z 2017-11- 12T23:59:59.000Z 208.11.141.128 443 billerops- beta.nc.checkfree.co m GeoTrust, Inc. 2012-04- 08T20:46:41.000Z 2014-04- 12T04:43:20.000Z 208.11.141.77 443 sponsorcare- alpha.nc.checkfree.co m GeoTrust Inc. 2016-02- 19T15:22:11.000Z 2018-02- 19T15:22:11.000Z 208.11.141.177 443 beta- yes.checkfree.com Equifax 2008-08- 19T15:22:11.000Z 2010-10- 19T15:22:11.000Z 208.11.141.177 443 bofa- alpha.nc.checkfree.co m GeoTrust Inc. 2016-02- 22T00:00:00.000Z 2018-02- 21T23:59:59.000Z 208.11.141.157 443	•	GeoTrust Inc.			192.131.76.61	443
alphanc.checkfree.com 20T07:32:54.000Z 21T20:40:55.000Z alphaaps.checkfree.com GeoTrust Inc. 2015-11- 13T00:00:00.000Z 2017-11- 12T23:59:59.000Z 208.11.141.128 443 billerops-beta.nc.checkfree.com GeoTrust, Inc. 2012-04- 08T20:46:41.000Z 2014-04- 12T04:43:20.000Z 208.11.141.77 443 sponsorcare-alpha.nc.checkfree.com GeoTrust Inc. 2016-02- 02T00:00:00.000Z 2018-02- 01T23:59:59.000Z 208.11.141.77 443 beta-yes.checkfree.com Equifax 2008-08- 19T15:22:11.000Z 2010-10- 19T15:22:11.000Z 208.11.141.177 443 bofa-alpha.nc.checkfree.com GeoTrust Inc. 2016-02- 22T00:00:00.000Z 2018-02- 21T23:59:59.000Z 208.11.141.157 443		GeoTrust Inc.			50.58.9.223	443
aps.checkfree.com 13T00:00:00.000Z 12T23:59:59.000Z billerops-beta.nc.checkfree.co m Sponsorcare-alpha.nc.checkfree.co m Equifax 2008-08-19T15:22:11.000Z 19T15:22:11.000Z 208.11.141.177 443 beta-yes.checkfree.co m GeoTrust Inc. 2016-02- 2018-02- 208.11.141.73 443 2008-08- 19T15:22:11.000Z 19T15:22:11.000Z 208.11.141.177 443	alpha.nc.checkfree.co	GeoTrust, Inc.			208.11.141.74	443
beta.nc.checkfree.co m Sponsorcare- alpha.nc.checkfree.co m Equifax Deta- yes.checkfree.com Defa- alpha.nc.checkfree.co m Sponsorcare- alpha.nc.checkfree.co m Equifax Deta- yes.checkfree.com Deta- yes.checkfree.co	•	GeoTrust Inc.			208.11.141.128	443
alpha.nc.checkfree.co m 02T00:00:00:00.000Z 01T23:59:59.000Z beta- yes.checkfree.com Equifax 19T15:22:11.000Z 2010-10- 208.11.141.177 443 bofa- alpha.nc.checkfree.co m GeoTrust Inc. 2016-02- 22T00:00:00.000Z 2018-02- 2018-02- 21T23:59:59.000Z 208.11.141.157 443	beta.nc.checkfree.co	GeoTrust, Inc.			208.11.141.77	443
yes.checkfree.com 19T15:22:11.000Z 19T15:22:11.000Z bofa- GeoTrust Inc. 2016-02- 2018-02- 208.11.141.157 443 alpha.nc.checkfree.co 22T00:00:00.000Z 21T23:59:59.000Z	alpha.nc.checkfree.co	GeoTrust Inc.			208.11.141.73	443
alpha.nc.checkfree.co 22T00:00:00.000Z 21T23:59:59.000Z m		Equifax			208.11.141.177	443
adapters- GeoTrust Inc. 2016-05- 2018-05- 208.11.141.84 443	alpha.nc.checkfree.co	GeoTrust Inc.			208.11.141.157	443
	adapters-	GeoTrust Inc.	2016-05-	2018-05-	208.11.141.84	443

alpha.nc.checkfree.co m		26T00:00:00.000Z	26T23:59:59.000Z		
ebilldetaildownload- beta.nc.checkfree.co m	Checkfree Corp.	2006-03- 22T19:40:35.000Z	2011-03- 21T19:40:35.000Z	208.11.141.167	443
sgpgw02.cbs.fiserv.co m	GeoTrust Inc.	2016-10- 26T00:00:00.000Z	2018-10- 26T23:59:59.000Z	203.120.42.194	443
*.billmatrix.com	BMC Production	2016-01- 07T20:01:31.000Z	2018-09- 17T17:21:56.000Z	166.73.102.182	443
monetise- services.onefiserv.co m	GeoTrust, Inc.	2014-10- 13T11:29:40.000Z	2016-11- 13T23:02:04.000Z	208.235.248.43	443
*.billmatrix.com	BMC Production	2016-01- 07T20:01:31.000Z	2018-09- 17T17:21:56.000Z	166.73.102.190	443
connectdublin.checkfr ee.com	GeoTrust, Inc.	2013-08- 25T18:37:44.000Z	2015-09- 28T05:29:27.000Z	12.16.164.65	443
dr.fiservipvpn.com	Symantec Corporation	2015-03- 27T00:00:00.000Z	2016-03- 27T23:59:59.000Z	65.213.167.2	443
billerdirect.onefiserv.c	GeoTrust, Inc.	2014-04- 13T01:50:37.000Z	2015-07- 29T06:06:06.000Z	64.128.99.48	443
iclyncpool01.corp.che ckfree.com	GeoTrust, Inc.	2012-06- 10T08:28:05.000Z	2016-06- 12T08:10:33.000Z	204.95.150.234	443
datadelivery- cert.onefiserv.com	GeoTrust, Inc.	2015-04- 06T15:14:30.000Z	2016-06- 07T16:50:11.000Z	12.168.132.202	443
mmscts- beta.checkfree.com	GeoTrust, Inc.	2012-03- 11T23:20:27.000Z	2014-03- 15T13:42:38.000Z	12.168.133.87	443
achasp1- btat2.fiserv.com	Trustwave Holdings, Inc.	2014-12- 09T04:49:01.000Z	2016-12- 08T10:49:01.000Z	12.168.133.174	443
mcc-tgo01- btat2.mybills.com	GeoTrust Inc.	2016-06- 14T00:00:00.000Z	2018-06- 14T23:59:59.000Z	12.168.133.240	443
mcc-tgo01- btat2.mybills.com	GeoTrust Inc.	2016-06- 14T00:00:00.000Z	2018-06- 14T23:59:59.000Z	12.168.133.236	443
dit1-cardvalet- m.fiservapps.com	GeoTrust Inc.	2015-12- 11T00:00:00.000Z	2017-12- 10T23:59:59.000Z	166.73.13.211	443
dit1-cardvalet- ws.fiservapps.com	GeoTrust Inc.	2015-12- 11T00:00:00.000Z	2017-12- 10T23:59:59.000Z	166.73.13.212	443
dit1-cardvalet- mobiliti.fiservapps.co m	GeoTrust Inc.	2015-12- 11T00:00:00.000Z	2017-12- 10T23:59:59.000Z	166.73.13.210	443
mobile-lic01- uat.fiservapps.com	GeoTrust Inc.	2016-03- 11T00:00:00.000Z	2018-03- 11T23:59:59.000Z	166.73.13.93	443
services1.fiserv.com	GeoTrust, Inc.	2015-04- 15T06:42:25.000Z	2016-05- 17T01:23:06.000Z	50.58.9.181	443
merchantselfcare.che ckfree.com	GeoTrust Inc.	2016-10- 24T00:00:00.000Z	2018-10- 24T23:59:59.000Z	63.251.77.66	443

*.onefiserv.com	GeoTrust Inc.	2016-01- 12T00:00:00.000Z	2018-01- 11T23:59:59.000Z	64.128.99.136	443
services- prod.onefiserv.com	GeoTrust Inc.	2016-03- 24T00:00:00.000Z	2018-03- 24T23:59:59.000Z	64.128.99.151	443
*.onefiserv.com	GeoTrust Inc.	2016-01- 12T00:00:00.000Z	2018-01- 11T23:59:59.000Z	64.128.99.68	443
merchantselfcare.che ckfree.com	GeoTrust Inc.	2016-10- 24T00:00:00.000Z	2018-10- 24T23:59:59.000Z	64.128.99.84	443
webmail.fiserv.net	GeoTrust, Inc.	2012-04- 10T09:02:40.000Z	2017-01- 13T20:39:20.000Z	204.95.150.230	443
*.billmatrix.com	BMC Production	2016-01- 07T20:01:31.000Z	2018-09- 17T17:21:56.000Z	166.73.156.142	443
*.billmatrix.com	BMC Production	2016-01- 07T20:01:31.000Z	2018-09- 17T17:21:56.000Z	166.73.156.150	443
qc- emoney.checkfree.co m	GeoTrust Inc.	2015-06- 10T00:00:00.000Z	2017-06- 09T23:59:59.000Z	208.11.141.192	443
wbp321- beta.nc.checkfree.co m	Checkfree Corp.	2003-11- 04T19:48:18.000Z	2003-12- 04T19:48:18.000Z	208.11.141.196	443
onboardadvisor.app.fi serv.com	GeoTrust Inc.	2016-07- 19T00:00:00.000Z	2018-07- 19T23:59:59.000Z	50.58.9.141	443
download- secure.wealthmanage mentbackup.fiserv.co	GeoTrust, Inc.	2013-12- 07T05:09:02.000Z	2016-01- 08T22:13:59.000Z	209.211.226.237	443
m					
•	GeoTrust, Inc.	2013-11- 16T13:20:32.000Z	2016-01- 18T06:03:12.000Z	209.211.226.236	443
m secure.wealthmanage mentbackup.fiserv.co	GeoTrust, Inc. Trustwave Holdings, Inc.			209.211.226.236 170.90.16.202	443
m secure.wealthmanage mentbackup.fiserv.co m proposalgenerationm anager.fiservapps.co	Trustwave Holdings,	16T13:20:32.000Z	18T06:03:12.000Z		
m secure.wealthmanage mentbackup.fiserv.co m proposalgenerationm anager.fiservapps.co m connectnorcross.fiser	Trustwave Holdings, Inc.	16T13:20:32.000Z 2015-05- 18T06:50:18.000Z	18T06:03:12.000Z 2017-05- 17T12:50:18.000Z	170.90.16.202	443
m secure.wealthmanage mentbackup.fiserv.co m proposalgenerationm anager.fiservapps.co m connectnorcross.fiser v.com mcom-asp-	Trustwave Holdings, Inc. GeoTrust, Inc.	16T13:20:32.000Z 2015-05- 18T06:50:18.000Z 2010-08- 24T09:07:00.000Z	18T06:03:12.000Z 2017-05- 17T12:50:18.000Z 2012-09- 24T21:23:22.000Z	170.90.16.202 204.95.150.47	443 443
m secure.wealthmanage mentbackup.fiserv.co m proposalgenerationm anager.fiservapps.co m connectnorcross.fiser v.com mcom-asp- btat.onefiserv.com mcom-asp-	Trustwave Holdings, Inc. GeoTrust, Inc. GeoTrust Inc.	16T13:20:32.000Z 2015-05- 18T06:50:18.000Z 2010-08- 24T09:07:00.000Z 2016-09- 21T00:00:00.000Z	18T06:03:12.000Z 2017-05- 17T12:50:18.000Z 2012-09- 24T21:23:22.000Z 2018-09- 21T23:59:59.000Z	170.90.16.202 204.95.150.47 192.131.76.58	443 443 443
m secure.wealthmanage mentbackup.fiserv.co m proposalgenerationm anager.fiservapps.co m connectnorcross.fiser v.com mcom-asp- btat.onefiserv.com director-ipad-	Trustwave Holdings, Inc. GeoTrust, Inc. GeoTrust Inc. GeoTrust Inc.	16T13:20:32.000Z 2015-05- 18T06:50:18.000Z 2010-08- 24T09:07:00.000Z 2016-09- 21T00:00:00.000Z 2016-09- 21T00:00:00.000Z	18T06:03:12.000Z 2017-05- 17T12:50:18.000Z 2012-09- 24T21:23:22.000Z 2018-09- 21T23:59:59.000Z 2018-09- 21T23:59:59.000Z	170.90.16.202 204.95.150.47 192.131.76.58 192.131.76.60	443443443443
m secure.wealthmanage mentbackup.fiserv.co m proposalgenerationm anager.fiservapps.co m connectnorcross.fiser v.com mcom-asp- btat.onefiserv.com director-ipad- qa.fiservapps.com mcom-asp- mcom-asp- mcom-asp- mcom-asp- mcom-asp- mcom-asp- mcom-asp- mcom-asp-	Trustwave Holdings, Inc. GeoTrust, Inc. GeoTrust Inc. GeoTrust Inc. GeoTrust, Inc.	16T13:20:32.000Z 2015-05- 18T06:50:18.000Z 2010-08- 24T09:07:00.000Z 2016-09- 21T00:00:00.000Z 2013-10- 24T14:06:12.000Z	18T06:03:12.000Z 2017-05- 17T12:50:18.000Z 2012-09- 24T21:23:22.000Z 2018-09- 21T23:59:59.000Z 2018-09- 21T23:59:59.000Z 2015-10- 27T09:22:58.000Z	170.90.16.202 204.95.150.47 192.131.76.58 192.131.76.60 192.131.76.40	443 443 443 443

uat2.onefiserv.com		09T00:00:00.000Z	09T23:59:59.000Z		
*.onefiserv.com	GeoTrust Inc.	2016-01- 12T00:00:00.000Z	2018-01- 11T23:59:59.000Z	192.131.46.180	443
b2b.elending.fiservlen dingsolutions.com	GeoTrust Inc.	2015-09- 18T00:00:00.000Z	2017-09- 17T23:59:59.000Z	192.131.46.150	443
www.bankintelligence .fiserv.com	Symantec Corporation	2015-06- 01T00:00:00.000Z	2018-05- 26T23:59:59.000Z	64.74.244.77	443
*.fiservapps.com	GeoTrust Inc.	2015-06- 23T00:00:00.000Z	2017-06- 22T23:59:59.000Z	209.163.213.156	443
partnercare- beta.nc.checkfree.co m	GeoTrust, Inc.	2012-09- 13T06:17:38.000Z	2014-09- 15T10:41:24.000Z	208.11.141.88	443
reports.checkfree.co m	Equifax	2006-05- 18T16:10:44.000Z	2008-05- 18T16:10:44.000Z	12.16.165.87	443
monetise- services.onefiserv.co m	GeoTrust, Inc.	2014-10- 13T11:29:40.000Z	2016-11- 13T23:02:04.000Z	12.16.165.142	443
oa-mc- dr.onefiserv.com	GeoTrust, Inc.	2012-02- 26T21:34:09.000Z	2014-03- 01T08:28:56.000Z	12.16.165.108	443
*.fiservse.com	GlobalSign nv-sa	2015-08- 28T17:01:02.000Z	2017-08- 28T17:01:02.000Z	65.210.130.84	443
*.onefiserv.com	GeoTrust Inc.	2016-01- 12T00:00:00.000Z	2018-01- 11T23:59:59.000Z	12.16.165.109	443
pacific- uat.hepsiian.com	GeoTrust, Inc.	2013-04- 15T16:10:14.000Z	2015-04- 18T17:11:51.000Z	64.149.172.133	443
services1.fiserv.com	GeoTrust Inc.	2016-04- 01T00:00:00.000Z	2018-04- 01T23:59:59.000Z	64.128.99.60	443
uhgapps.hepsiian.co m	GeoTrust, Inc.	2013-09- 08T18:04:31.000Z	2015-11- 10T18:09:52.000Z	64.149.172.162	443
nascodrs.hepsiian.co m	GeoTrust Inc.	2015-11- 20T00:00:00.000Z	2017-11- 19T23:59:59.000Z	64.149.171.19	443
*.fiservse.com	GlobalSign nv-sa	2015-08- 28T17:01:02.000Z	2017-08- 28T17:01:02.000Z	65.210.130.82	443

RECOMMENDATION

Services presenting expired certificates should cause noticeable failures, so confirm the service is still in use. If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate, while ensuring the clients that use the service are configured to validate certificates when making TLS connections. If the clients were configured to validate certificates, ensure that their errors are monitored. Evaluate the organization's certificate management policy to ensure that certificates are renewed or decommissioned prior to their expiration date.

ABOUT THIS ISSUE

When a Certificate Authority (CA) issues a certificate, they embed two dates: the date at which the certificate starts being valid, and the date at which the certificate stops being valid. If the certificate a TLS server (e.g., website) presents to a client (e.g., web browser) is outside of those two dates, the client will refuse to connect to the server. Certificates are digital assets that require renewal or decommissioning on a schedule.

NETWORK SECURITY > ISSUE DETAIL

Certificate Is Self-Signed

Servers presenting self-signed certificates trigger warnings in, or prevent connections from TLS clients.

-0.2 SCORE

2 findings

SUBJECT COMMON NAME	ISSUER ORGANIZATION NAME	NOT VALID BEFORE	NOT VALID AFTER	DESTINATION IP	DESTINATION PORT
bac-saml- prod.fiservapps.com	Fiserv	2018-09- 13T17:35:23.000Z	2019-09- 13T17:35:23.000Z	208.235.248.133	443
efichwaf660a- 59.Fiserv.com	Fiserv	2017-12- 07T22:05:25.000Z	2020-12- 06T22:05:25.000Z	216.138.118.59	443

RECOMMENDATION

Services presenting self-signed certificates should cause noticeable failures or user-visible warnings, so confirm the service is still in use. If the service is not in use, decommission it. Otherwise, contact your CA and arrange issuance of a new certificate, while ensuring the clients that use the service are configured to validate certificates when making TLS connections. If the clients were configured to validate certificates, ensure that their errors are monitored.

ABOUT THIS ISSUE

When a certificate is issued, it is 'signed' by a certificate authority (CA). Signatures are attestations of the certificate-holder's identity. TLS clients (e.g., web browsers) maintain trust stores, which are lists of CAs whose attestations they trust. The ability to sign a certificate may be delegated from a CA to another entity, such as a subsidiary, creating chains of attestations. In the context of chains of attestation, the delegating CA is the root CA, and the delegated CA is the intermediate CA. Trust stores in TLS clients may contain both intermediate and root CAs. TLS clients validate a server's certificate by tracing its chain of attestations back to a CA in its trust store. Certificates that are self-signed have no chain of attestations: they are self-attested. This means that most TLS clients, when presented with a selfsigned certificate, will display a warning before connecting to the server, or refuse to connect to the server. Off-the-shelf software and hardware frequently runs services that use selfsigned certificates by default. Many of these services can be configured to use certificates that are not self-signed. The use of self-signed certificates may result in TLS clients being configured to skip validating certificates, making their connections vulnerable to man-in-the-middle attacks. Users that bypass their web browser's warning upon connecting to a server presenting a self-signed certificate are also vulnerable to manin-the-middle attacks. Self-signed certificates have narrow, but legitimate use cases, such as protecting services whose clients are configured to use public key pinning.

NETWORK SECURITY > ISSUE DETAIL



TLS analysis reveals a weak signature algorithms, using SHA1 or MD5.

-0.7 SCORE

24 findings

IMPACT

24 findings					
SUBJECT COMMON NAME	ISSUER ORGANIZATION NAME	NOT VALID BEFORE	NOT VALID AFTER	DESTINATION IP	DESTINATION PORT
*.lending.fiservapps.c om	GeoTrust, Inc.	2013-09- 04T11:10:54.000Z	2017-09- 06T05:06:26.000Z	198.246.154.33	443
connectdublin.checkfr ee.com	GeoTrust, Inc.	2013-08- 25T18:37:44.000Z	2015-09- 28T05:29:27.000Z	12.16.164.65	443
connectnorcross.fiser v.com	GeoTrust, Inc.	2010-08- 24T09:07:00.000Z	2012-09- 24T21:23:22.000Z	204.95.150.47	443
ebilldetaildownload- beta.nc.checkfree.co m	Checkfree Corp.	2006-03- 22T19:40:35.000Z	2011-03- 21T19:40:35.000Z	208.11.141.167	443
connectdublin.checkfr ee.com	GeoTrust, Inc.	2013-08- 25T18:37:44.000Z	2015-09- 28T05:29:27.000Z	12.16.164.14	443
*.billmatrix.com	BMC Production	2016-01- 07T20:01:31.000Z	2018-09- 17T17:21:56.000Z	166.73.156.142	443
billerops- alpha.nc.checkfree.co m	GeoTrust, Inc.	2012-02- 20T07:32:54.000Z	2014-02- 21T20:40:55.000Z	208.11.141.74	443
services1.fiserv.com	GeoTrust, Inc.	2015-04- 15T06:42:25.000Z	2016-05- 17T01:23:06.000Z	50.58.9.181	443
pacific- uat.hepsiian.com	GeoTrust, Inc.	2013-04- 15T16:10:14.000Z	2015-04- 18T17:11:51.000Z	64.149.172.189	443
download- secure.wealthmanage mentbackup.fiserv.co m	GeoTrust, Inc.	2013-12- 07T05:09:02.000Z	2016-01- 08T22:13:59.000Z	209.211.226.237	443
oa-mc- dr.onefiserv.com	GeoTrust, Inc.	2012-02- 26T21:34:09.000Z	2014-03- 01T08:28:56.000Z	12.16.165.108	443
pacific- uat.hepsiian.com	GeoTrust, Inc.	2013-04- 15T16:10:14.000Z	2015-04- 18T17:11:51.000Z	64.149.172.133	443
reports.checkfree.co m	Equifax	2006-05- 18T16:10:44.000Z	2008-05- 18T16:10:44.000Z	12.16.165.87	443
alpha- merchantselfcare.che ckfree.com	Equifax	2008-10- 17T14:35:55.000Z	2010-11- 17T15:35:55.000Z	208.11.141.178	443
billerdirect.onefiserv.c om	GeoTrust, Inc.	2014-04- 13T01:50:37.000Z	2015-07- 29T06:06:06.000Z	64.128.99.48	443
monetise- services.onefiserv.co m	GeoTrust, Inc.	2014-10- 13T11:29:40.000Z	2016-11- 13T23:02:04.000Z	12.16.165.142	443
uhgapps.hepsiian.co m	GeoTrust, Inc.	2013-09- 08T18:04:31.000Z	2015-11- 10T18:09:52.000Z	64.149.172.162	443
monetise-	GeoTrust, Inc.	2014-10-	2016-11-	208.235.248.43	443

services.onefiserv.co m		13T11:29:40.000Z	13T23:02:04.000Z		
mmscts- beta.checkfree.com	GeoTrust, Inc.	2012-03- 11T23:20:27.000Z	2014-03- 15T13:42:38.000Z	12.168.133.87	443
*.billmatrix.com	BMC Production	2016-01- 07T20:01:31.000Z	2018-09- 17T17:21:56.000Z	166.73.102.182	443
*.lending.fiservapps.c om	GeoTrust, Inc.	2013-09- 04T11:10:54.000Z	2017-09- 06T05:06:26.000Z	192.131.76.225	443
beta- yes.checkfree.com	Equifax	2008-08- 19T15:22:11.000Z	2010-10- 19T15:22:11.000Z	208.11.141.177	443
webmail.fiserv.net	GeoTrust, Inc.	2012-04- 10T09:02:40.000Z	2017-01- 13T20:39:20.000Z	204.95.150.230	443
director-ipad- qa.fiservapps.com	GeoTrust, Inc.	2013-10- 24T14:06:12.000Z	2015-10- 27T09:22:58.000Z	192.131.76.40	443

RECOMMENDATION

Contact the authority that manages your SSL Certification to ensure that you have an updated signature—such as SHA-2.

ABOUT THIS ISSUE

The integrity of the signature hash algorithm used in signing a certificate is a critical element in the security of the certificate. Weaknesses in hash algorithms can lead to situations in which attackers can obtain fraudulent certificates. The MD5 signature has long been considered outdated by cryptographic specialists. SHA-1 is outdated and has been phased out by several sources including Microsoft, Google, and Mozilla as of January 1, 2016.

NETWORK SECURITY > ISSUE DETAIL

TLS Protocol Uses Weak Cipher

TLS analysis reveals a weak cipher either through encryption protocol or public key length.

-0.5 SCORE

33 findings

SUBJECT COMMON NAME	ISSUER ORGANIZATION NAME	NOT VALID BEFORE	NOT VALID AFTER	DESTINATION IP	DESTINATION PORT
dalvdmz37.carreker.c om	Symantec Corporation	2017-09- 08T00:00:00.000Z	2019-09- 09T23:59:59.000Z	209.163.213.137	443
connectdublin.checkfr ee.com	GeoTrust, Inc.	2013-08- 25T18:37:44.000Z	2015-09- 28T05:29:27.000Z	12.16.164.65	443
architectbk.onefiserv.	DigiCert Inc	2018-11- 21T00:00:00.000Z	2020-11- 21T12:00:00.000Z	184.170.226.96	443
SysAdmin7- Prod.fiservapps.com	DigiCert Inc	2018-08- 08T00:00:00.000Z	2020-08- 08T12:00:00.000Z	192.131.72.142	443
connectnorcross.fiser v.com	GeoTrust, Inc.	2010-08- 24T09:07:00.000Z	2012-09- 24T21:23:22.000Z	204.95.150.47	443
*.fiservse.com	GlobalSign nv-sa	2017-06- 30T12:36:04.000Z	2020-06- 30T12:36:04.000Z	12.168.17.230	443

connectdublin.checkfr ee.com	GeoTrust, Inc.	2013-08- 25T18:37:44.000Z	2015-09- 28T05:29:27.000Z	12.16.164.14	443
sydgw01.cbs.fiserv.co m	GeoTrust Inc.	2017-01- 05T00:00:00.000Z	2019-01- 05T23:59:59.000Z	210.50.55.217	443
achcpo- dr.onefiserv.com	DigiCert Inc	2018-08- 21T00:00:00.000Z	2020-08- 21T12:00:00.000Z	50.58.9.212	443
sgpgw01.cbs.fiserv.co m	GeoTrust Inc.	2017-01- 05T00:00:00.000Z	2019-01- 05T23:59:59.000Z	210.24.157.4	443
*.billmatrix.com	BMC Production	2016-01- 07T20:01:31.000Z	2018-09- 17T17:21:56.000Z	166.73.156.142	443
orlgw01.cbs.fiserv.co m	GeoTrust Inc.	2017-01- 05T00:00:00.000Z	2019-01- 05T23:59:59.000Z	205.160.248.202	443
nyl.hepsiian.com	DigiCert Inc	2018-03- 07T00:00:00.000Z	2020-03- 07T12:00:00.000Z	64.149.172.70	443
sgpgw01.cbs.fiserv.co m	GeoTrust Inc.	2017-01- 05T00:00:00.000Z	2019-01- 05T23:59:59.000Z	210.24.157.3	443
download- secure.wealthmanage mentbackup.fiserv.co m	GeoTrust, Inc.	2013-12- 07T05:09:02.000Z	2016-01- 08T22:13:59.000Z	209.211.226.237	443
secure.wealthmanage mentbackup.fiserv.co m	Symantec Corporation	2017-05- 15T00:00:00.000Z	2019-05- 16T23:59:59.000Z	50.58.9.169	443
reports.checkfree.co m	Equifax	2006-05- 18T16:10:44.000Z	2008-05- 18T16:10:44.000Z	12.16.165.87	443
otms.fiserv.com	DigiCert Inc	2018-08- 17T00:00:00.000Z	2020-08- 17T12:00:00.000Z	63.128.95.117	443
sydgw01.cbs.fiserv.co m	GeoTrust Inc.	2017-01- 05T00:00:00.000Z	2019-01- 05T23:59:59.000Z	210.50.55.210	443
www.rbscashorderts.fi serv.com	Symantec Corporation	2017-04- 04T00:00:00.000Z	2019-04- 05T23:59:59.000Z	204.97.230.108	443
achrwa.checkfree.co m	DigiCert Inc	2018-01- 03T00:00:00.000Z	2020-01- 04T12:00:00.000Z	12.16.165.127	443
secure.wealthmanage mentprimary.fiserv.co m	Symantec Corporation	2017-05- 17T00:00:00.000Z	2019-05- 18T23:59:59.000Z	166.73.6.60	443
awdmg.fiserv.com	DigiCert Inc	2018-01- 23T00:00:00.000Z	2020-01- 24T12:00:00.000Z	50.58.10.132	443
ondemand.fiserv.com	DigiCert Inc	2017-12- 14T00:00:00.000Z	2019-12- 15T12:00:00.000Z	204.95.150.37	443
awmag.fiserv.com	DigiCert Inc	2018-01- 23T00:00:00.000Z	2020-01- 24T12:00:00.000Z	204.95.150.239	443
awseg.fiserv.com	DigiCert Inc	2018-01- 23T00:00:00.000Z	2020-01- 24T12:00:00.000Z	204.95.150.240	443
SFTM2.Premier.Fiserv	DigiCert Inc	2018-04-	2020-04-	192.131.55.67	443

.com		27T00:00:00.000Z	27T12:00:00.000Z		
Inkvpn.fiserv.com	Symantec Corporation	2017-01- 26T00:00:00.000Z	2020-01- 27T23:59:59.000Z	98.19.116.50	443
SFTM.Premier.Fiserv.c om	Symantec Corporation	2017-07- 17T00:00:00.000Z	2019-07- 18T23:59:59.000Z	192.131.55.66	443
otms.fiserv.com	DigiCert Inc	2018-08- 17T00:00:00.000Z	2020-08- 17T12:00:00.000Z	205.219.236.229	443
*.fiservapps.com	Symantec Corporation	2017-07- 10T00:00:00.000Z	2019-07- 11T23:59:59.000Z	166.73.6.105	443
director-ipad- qa.fiservapps.com	GeoTrust, Inc.	2013-10- 24T14:06:12.000Z	2015-10- 27T09:22:58.000Z	192.131.76.40	443
longw01.cbs.fiserv.co m	GeoTrust Inc.	2017-01- 05T00:00:00.000Z	2019-01- 05T23:59:59.000Z	89.197.167.78	443

It is recommended to configure the server to only support strong symmetric ciphers and to use sufficiently large public key sizes. Specifically, avoid RC4 encryption as there have been multiple vulnerabilities discovered that render it insecure. Additionally, it is recommended to use a public key size of more than 2048 bits.

ABOUT THIS ISSUE

The TLS cryptographic configuration being used could be defeated. A symmetric cipher suite is specified by an encryption protocol (e.g. DES, AES). The strength of the encryption used within a Transport Layer Security (TLS) session is determined by the encryption symmetric cipher negotiated between the server and the browser. In order to ensure that only strong cryptographic ciphers are selected the server must be modified to disable the use of weak ciphers and to configure the ciphers in an adequate order. Additionally, as part of the TLS handshake, an asymmetric cipher is utilized. The strength of the asymmetric cipher may be weakened if an insufficient key size is selected.

NETWORK SECURITY > ISSUE DETAIL

FTP Service Observed

We observed FTP, a file-sharing service, publicly exposed.

-0.1 SCORE IMPACT

51 findings

PRODUCT	NAME PRODUCT V	ERSION DESTINATION IF	DESTINATION P	ORT LAST SEEN
oftpd	-	198.167.0.222	990	2019-01-20T16:34:41.000Z
oftpd	-	198.167.0.71	990	2019-01-20T16:34:01.000Z
oftpd	-	198.167.0.175	990	2019-01-20T16:32:44.000Z
oftpd	-	198.167.0.172	990	2019-01-20T16:31:39.000Z
oftpd	-	198.167.0.223	990	2019-01-20T16:31:30.000Z
oftpd	-	198.167.0.25	990	2019-01-20T16:24:59.000Z
oftpd	-	198.167.0.173	990	2019-01-20T16:17:31.000Z

oftpd	-	198.167.0.73	990	2019-01-20T16:16:48.000Z
oftpd	-	198.167.0.171	990	2019-01-20T15:37:05.000Z
oftpd	-	198.167.0.72	990	2019-01-20T15:36:43.000Z
oftpd	-	198.167.0.51	990	2019-01-20T15:11:57.000Z
oftpd	-	198.167.0.72	21	2019-01-12T20:49:31.100Z
Banner: 220 Service ready for new	user.\r\n			
oftpd	-	198.167.0.25	21	2019-01-12T20:37:01.486Z
Banner: 220 Service ready for new	user.\r\n			
oftpd	-	198.167.0.64	21	2019-01-12T20:24:58.142Z
Banner: 220 Service ready for new	user.\r\n			
-	-	65.213.167.45	21	2019-01-12T20:20:04.143Z
Authorized users may\r\n22	20-be restricted to certain function		0-responsibilities. Any un	roper authorization by Fiserv and its affiliates. authorized access will be investigated and er, disconnect now.\r\n
oftpd	-	198.167.0.222	21	2019-01-12T20:00:25.579Z
Banner: 220 Service ready for new	user.\r\n			
Microsoft ftpd	-	50.58.8.116	21	2019-01-12T19:31:45.998Z
Banner: 220 Microsoft FTP Service\	r\n			
-	-	65.213.167.80	21	2019-01-12T19:24:11.313Z
Authorized users may\r\n22	20-be restricted to certain function	mputer system. Access is restricted ns in accordance with their job\r\n22 ding criminal\r\n220 sanctions. If you	0-responsibilities. Any un	er authorization by Fiserv and its affiliates. authorized access will be investigated and er, disconnect now.\r\n
oftpd	-	198.167.0.176	21	2019-01-12T19:08:52.369Z
Banner: 220 Service ready for new	user.\r\n			
ProFTPD	-	208.235.248.3	21	2019-01-12T18:03:47.304Z
Banner: 220 65.167.147.52 FTP serv	ver ready\r\n			
oftpd	-	198.167.0.223	21	2019-01-12T17:31:35.078Z
Banner: 220 Service ready for new	user.\r\n			
oftpd	-	198.167.0.175	21	2019-01-12T17:11:59.204Z
Banner: 220 Service ready for new	user.\r\n			
oftpd	-	198.167.0.179	21	2019-01-12T17:05:57.019Z

Banner:	v voor lela			
220 Service ready for new	v user.\r\n			
Microsoft ftpd	-	50.58.8.117	21	2019-01-12T16:48:41.935Z
Banner:				
220 Microsoft FTP Service	e\r\n			
oftpd	_	198.167.0.63	21	2019-01-12T16:45:25.456Z
onpu		130.107.0.00	2.	2013 01 12110: 10:20: 1002
Banner: 220 Service ready for new	v user.\r\n			
oftpd	-	198.167.0.65	21	2019-01-12T16:41:03.192Z
Banner: 220 Service ready for new	v user.\r\n			
oftpd	-	198.167.0.180	21	2019-01-12T16:30:04.420Z
Banner: 220 Service ready for new	v user \r\n			
zzo cerrice reday rer ner	. 400			
oftpd	-	198.167.0.67	21	2019-01-12T16:10:38.358Z
Banner: 220 Service ready for new	v user.\r\n			
Pure-FTPd	-	209.221.136.222	21	2019-01-12T16:07:01.089Z
				e is now 08:06. Server port: 21.\r\n220-This is a nnected after 15 minutes of inactivity.\r\n
oftpd	-	198.167.0.70	21	2019-01-12T16:05:30.825Z
Banner: 220 Service ready for new	v user.\r\n			
oftpd	-	198.167.0.124	21	2019-01-12T15:54:34.710Z
Banner: 220 Service ready for new	v user.\r\n			
oftpd	-	198.167.0.113	21	2019-01-12T15:32:32.323Z
Banner: 220 Service ready for new	v user.\r\n			
oftpd	-	198.167.0.73	21	2019-01-12T15:23:52.975Z
Banner: 220 Service ready for new	v user.\r\n			
oftpd	-	198.167.0.66	21	2019-01-12T14:59:01.080Z
Banner: 220 Service ready for new	v user.\r\n			
oftpd	-	198.167.0.177	21	2019-01-12T14:51:53.451Z
Banner: 220 Service ready for new	v user.\r\n			
oftpd	-	198.167.0.71	21	2019-01-12T14:19:50.894Z
Banner: 220 Service ready for new	v user.\r\n			
oftpd	-	198.167.0.174	21	2019-01-12T13:19:41.190Z

Banner: 220 Service ready for new user	:\r\n			
Gene6 ftpd	3.10.0 build 2	208.31.22.249	21	2019-01-12T13:16:28.523Z
Banner: 220 Gene6 FTP Server v3.10.0	(Build 2) ready\r\n			
oftpd	-	198.167.0.65	990	2018-12-20T11:21:30.000Z
oftpd	-	198.167.0.63	990	2018-12-20T11:21:17.000Z
oftpd	-	198.167.0.64	990	2018-12-20T11:18:50.000Z
oftpd	-	198.167.0.10	990	2018-12-20T11:18:41.000Z
-	-	65.213.167.80	990	2018-12-20T11:15:50.000Z
oftpd	-	198.167.0.151	990	2018-12-20T09:24:57.000Z
oftpd	-	198.167.0.113	990	2018-12-20T08:18:02.000Z
oftpd	-	198.167.0.70	990	2018-12-20T08:17:30.000Z
oftpd	-	198.167.0.124	990	2018-12-20T08:17:01.000Z
oftpd	-	198.167.0.174	990	2018-12-20T08:16:55.000Z
Serv-U ftpd	15.1	12.175.11.82	990	2018-12-20T07:29:34.000Z
oftpd	-	198.167.0.67	990	2018-12-20T07:27:24.000Z
oftpd	-	208.74.12.10	990	2018-12-20T06:50:41.000Z

Review the business necessity of hosting a public FTP server, and remove it from the Internet if possible. If not possible, consider restricting the service by whitelisting the IP addresses that require access.

ABOUT THIS ISSUE

The FTP protocol offers access to files stored on servers, giving users the ability to upload, download, and delete files. Many FTP servers are used by automated processes, and are neglected or poorly-configured. Modern protocols, such as SFTP, provide better security than FTP. We observed an FTP service on the Internet, accessible by the public. File-sharing services are attractive targets to attackers due to the data they may contain. An attacker that gains access to the files on an FTP server may sell the files within, use them for blackmail, or employ the information when launching further attacks. A breached FTP server may result in legal proceedings, have public notification requirements, negatively impact public image, and have insurance implications. Attackers may target the service with authentication bypass attacks (e.g., brute-forcing, buffer overflows, blank passwords) in an attempt to gain control of the host or exfiltrate its databases. Attackers may launch denial-ofservice (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL

Telnet Service Observed

We observed Telnet, a remote access service, publicly exposed.

-<0.1 SCORE

3 findings

PRODUCT NAME	PRODUCT VERSION	DESTINATION IP	DESTINATION PORT	LAST SEEN
Cisco router telnetd	-	12.111.185.1	23	2019-01-08T14:51:57.000Z
Cisco router telnetd	-	12.111.185.2	23	2019-01-08T14:51:08.000Z
Cisco router telnetd	-	12.111.185.3	23	2019-01-08T11:48:45.000Z

RECOMMENDATION

Telnet is an inherently unsafe protocol. Remove the service from the Internet. If a remote access service is necessary, replace Telnet with SSH if possible. If not possible, often the case with older networked hardware, ensure the service is only accessible by VPN.

ABOUT THIS ISSUE

Insecure and/or suspicious Telnet open ports have been detected as being publicly accessible. The availability of these ports allow attackers to engage in authentication bypass attacks (such as brute forcing attempts, remote buffer overflows, blank passwords). An attacker can leverage this access to pivot access into further enterprise resources.

NETWORK SECURITY > ISSUE DETAIL

Certificate Lifetime Is Longer Than Best Practices

We observed a certificate with a lifetime longer than 39 Months.

-0.1 SCORE IMPACT

6 findings

SUBJECT COMMON NAME	ISSUER ORGANIZATION NAME	NOT VALID BEFORE	NOT VALID AFTER	DESTINATION IP	DESTINATION PORT
*.lending.fiservapps.c om	GeoTrust, Inc.	2013-09- 04T11:10:54.000Z	2017-09- 06T05:06:26.000Z	198.246.154.33	443
*.lending.fiservapps.c om	GeoTrust, Inc.	2013-09- 04T11:10:54.000Z	2017-09- 06T05:06:26.000Z	192.131.76.225	443
ebilldetaildownload- beta.nc.checkfree.co m	Checkfree Corp.	2006-03- 22T19:40:35.000Z	2011-03- 21T19:40:35.000Z	208.11.141.167	443
iclyncpool01.corp.che ckfree.com	GeoTrust, Inc.	2012-06- 10T08:28:05.000Z	2016-06- 12T08:10:33.000Z	204.95.150.234	443
webmail.fiserv.net	GeoTrust, Inc.	2012-04- 10T09:02:40.000Z	2017-01- 13T20:39:20.000Z	204.95.150.230	443
aus-f5- 2000b.hs3.hepsiian.c om	Fiserv	2015-09- 16T20:06:57.000Z	2025-09- 13T20:06:57.000Z	64.149.172.32	443

Contact the CA and arrange the issuance of a new certificate with a lifetime that does not exceed 39 months.

ABOUT THIS ISSUE

When a Certificate Authority (CA) issues a certificate, they embed two dates: the date at which the certificate starts being valid, and the date at which the certificate stops being valid. If the certificate a TLS server (e.g., website) presents to a client (e.g., web browser) is outside of those two dates, the client will refuse to connect to the server. Cryptographic algorithms do not have a defined lifetime, but academics, researchers, and nation states are constantly evaluating them for weaknesses. New algorithms and versions of algorithms with larger key sizes are created regularly, and the best practices surrounding certificates evolve with them. The Certificate Authority and Browser forum, an industry group that sets standards surrounding the creation and use of certificates, has decided to limit the lifetime of certificates to 39 months. This means that CAs who are members of the forum are required to issue certificates with lifetimes that do not exceed 39 months.

NETWORK SECURITY > ISSUE DETAIL

TLS Certificate Without Revocation Control

We observed a TLS certificate that did not contain either CRL or OCSP URLs.

-<0.1 SCORE

5 findings

SUBJECT COMMON NAME	ISSUER ORGANIZATION NAME	NOT VALID BEFORE	NOT VALID AFTER	DESTINATION IP	DESTINATION PORT
ebilldetaildownload- beta.nc.checkfree.co m	Checkfree Corp.	2006-03- 22T19:40:35.000Z	2011-03- 21T19:40:35.000Z	208.11.141.167	443
bac-saml- prod.fiservapps.com	Fiserv	2018-09- 13T17:35:23.000Z	2019-09- 13T17:35:23.000Z	208.235.248.133	443
wbp321- beta.nc.checkfree.co m	Checkfree Corp.	2003-11- 04T19:48:18.000Z	2003-12- 04T19:48:18.000Z	208.11.141.196	443
efichwaf660a- 59.Fiserv.com	Fiserv	2017-12- 07T22:05:25.000Z	2020-12- 06T22:05:25.000Z	216.138.118.59	443
aus-f5- 2000b.hs3.hepsiian.c om	Fiserv	2015-09- 16T20:06:57.000Z	2025-09- 13T20:06:57.000Z	64.149.172.32	443

Contact the CA to request that the certificate be reissued with revocation controls.

ABOUT THIS ISSUE

Certificate revocation lists (CRLs) are files published online by certificate authorities (CAs). These lists indicate which certificates the CA has revoked, invalidating those certificates. TLS clients (e.g., web browsers) may download a CRL, referenced by a TLS server's certificate, to confirm the certificate is currently valid. CAs may operate online certificate status protocol (OCSP) servers, allowing TLS clients to query whether a certificate is currently valid. Responses to OCSP queries may be 'stapled to' (bundled with) certificates by TLS servers. OCSP stapling prevents TLS clients from needing to query the OCSP server themselves, resulting in faster TLS connections. If an attacker acquires the private key corresponding to a certificate, or any other breach of the private key occurs, the CA can use the revocation controls described above to inform TLS clients that the certificate is no longer valid. Certificates that do not contain revocation controls cannot be revoked, and if an attacker acquires the certificate's private key then the certificate will be valid until the expiry date.

NETWORK SECURITY > ISSUE DETAIL

Extended Validation Certificate Observed

The organization has undergone an extended identity-validation process when acquiring a certificate.

17 findings

SUBJECT COMMON NAME	ISSUER ORGANIZATION NAME	NOT VALID BEFORE	NOT VALID AFTER	DESTINATION IP	DESTINATION PORT
www.loancierge.galax y.app.fiserv.com	DigiCert Inc	2018-02- 13T00:00:00.000Z	2020-02- 14T12:00:00.000Z	198.246.218.225	443
www.loancierge.galax y.app.fiserv.com	DigiCert Inc	2018-02- 13T00:00:00.000Z	2020-02- 14T12:00:00.000Z	198.246.218.224	443
www.loancierge.galax y.app.fiserv.com	DigiCert Inc	2018-02- 13T00:00:00.000Z	2020-02- 14T12:00:00.000Z	198.246.218.226	443
www.netbranch.app.fi serv.com	DigiCert Inc	2018-10- 04T00:00:00.000Z	2020-10- 04T12:00:00.000Z	198.246.218.153	443
www.netbranch.app.fi serv.com	DigiCert Inc	2018-10- 04T00:00:00.000Z	2020-10- 04T12:00:00.000Z	198.246.218.157	443
www.netbranch.app.fi serv.com	DigiCert Inc	2018-10- 04T00:00:00.000Z	2020-10- 04T12:00:00.000Z	198.246.218.158	443
www.appscu.fiserv.co m	Symantec Corporation	2017-10- 19T00:00:00.000Z	2019-10- 20T23:59:59.000Z	198.246.218.81	443
www.netbranch.app.fi serv.com	DigiCert Inc	2018-10- 04T00:00:00.000Z	2020-10- 04T12:00:00.000Z	198.246.218.151	443
www.appscu.fiserv.co m	Symantec Corporation	2017-10- 19T00:00:00.000Z	2019-10- 20T23:59:59.000Z	198.246.218.83	443

www.netbranch.app.fi serv.com	DigiCert Inc	2018-10- 04T00:00:00.000Z	2020-10- 04T12:00:00.000Z	198.246.218.156	443
www.appscu.fiserv.co m	Symantec Corporation	2017-10- 19T00:00:00.000Z	2019-10- 20T23:59:59.000Z	198.246.218.82	443
accountcreate.fiserva pps.com	DigiCert Inc	2018-03- 15T00:00:00.000Z	2020-03- 15T12:00:00.000Z	198.246.218.72	443
www.netbranch.app.fi serv.com	DigiCert Inc	2018-10- 04T00:00:00.000Z	2020-10- 04T12:00:00.000Z	198.246.218.154	443
www.netbranch.app.fi serv.com	DigiCert Inc	2018-10- 04T00:00:00.000Z	2020-10- 04T12:00:00.000Z	198.246.218.152	443
accountcreate.fiserva pps.com	DigiCert Inc	2018-03- 15T00:00:00.000Z	2020-03- 15T12:00:00.000Z	198.246.218.70	443
accountcreate.fiserva pps.com	DigiCert Inc	2018-03- 15T00:00:00.000Z	2020-03- 15T12:00:00.000Z	198.246.218.71	443
evcms.hostbyweb.net	GlobalSign nv-sa	2018-03- 16T14:26:05.000Z	2019-12- 25T14:31:03.000Z	12.168.17.228	443

EV certificates should be strongly considered by organizations if their users are likely to be targeted by phishing attacks. Phishing attacks often use typosquatted domain names (e.g., exanple.com versus example.com). Users of legitimate sites, who are accustomed to the visual indicators associated with EV certificates are more likely to notice such attacks.

ABOUT THIS ISSUE

Certificate Authorities (CAs) issue certificates according to a variety of policies, and embed within each certificate a reference to the policy under which it was issued. The type of policy that offers the most assurance of the certificate-holder's identity is called an extended validation (EV) policy, and certificates issued under these policies are called EV certificates. To receive an EV certificate, an organization must prove to a CA that it is a currently-operating legal entity, along with several other attributes. EV certificates provide the highest level of assurance currently available. TLS clients (e.g., web browsers) consider EV certificates to be more trustworthy than certificates issued under other policies. Most web browsers display visual indicators a user is viewing a website secured with an EV certificate. Visual indicators provide additional assurance to the user that website they are viewing belongs to the company they intended to visit.

NETWORK SECURITY > ISSUE DETAIL

1 POP3 Service Observed

We observed POP3, an email retrieval service, publicly exposed.

2 findings

PRODUCT NAME	PRODUCT VERSION	DESTINATION IP	DESTINATION PORT	LAST SEEN
qpopper pop3d	-	208.66.20.24	995	2019-01-21T01:30:06.000Z
Dovecot pop3d	-	209.221.136.222	110	2018-12-25T21:09:08.772Z
Banner: +OK Dovecot ready.\r\n				

Review the business necessity of hosting a public POP3 server, and remove it from the Internet if possible. If not possible, consider restricting the service by whitelisting the IP addresses that require access.

ABOUT THIS ISSUE

The POP3 protocol offers access to messages stored on email servers. POP3 servers typically contain only the most recent messages received by an email account, deleting the messages from the server once they are downloaded by a user. The use of POP3 may complicate BCP/DR due to each individual user being responsible for the entirety of their email history. We observed a POP3 service on the Internet, accessible by the public. Email retrieval services are attractive targets to attackers due to the data they may contain. An attacker that gains access to an email account's messages may use them for blackmail, impersonating the owner of the email account, or employ the information when launching further attacks. An attacker with access to an email account's messages may gain access to many online accounts associated with that email address by using the password reset functions available on most websites. Attackers may target the service with authentication bypass attacks (e.g., brute-forcing, buffer overflows, blank passwords) in an attempt to gain control of the host or access the messages within. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.



ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

This module measures the health and configuration of a company's DNS settings. It validates that no malicious events occurred in the passive DNS history of the company's network. It also helps validate that mail servers have proper protection in place to avoid spoofing. It also helps verify that DNS servers are configured correctly.



DNS HEALTH > ISSUE DETAIL

SPF Record Missing

A missing SPF record has been detected for a domain.

-4.3 SCORE

102 findings

DOMAIN	LAST SEEN
fiservcbs.com	2019-01-30T23:51:39.156Z
fiserveft.net	2019-01-30T16:12:32.291Z
fiserveft.org	2019-01-30T16:11:38.752Z
fiserveasyweb.net	2019-01-30T16:11:22.208Z
fiserveft.com	2019-01-30T16:11:08.952Z
fiserveasyweb.com	2019-01-30T16:10:04.711Z
fiserve.com	2019-01-30T16:10:01.449Z
checkfreeweb.com	2019-01-30T15:37:44.766Z
onefiserv.org	2019-01-29T03:00:35.285Z
onefiserv.com	2019-01-29T02:55:31.305Z
fiservservices.info	2019-01-26T06:55:11.563Z
fiservsa2.com	2019-01-26T06:55:11.542Z
fiservdox.com	2019-01-26T06:55:11.494Z

fiservmail.com	2019-01-26T06:55:11.485Z
fiservfg.com	2019-01-26T06:55:11.428Z
zashpayfromfiserv.org	2019-01-26T06:55:10.576Z
fiserv.org	2019-01-26T06:55:10.572Z
zashpay-fiserv.org	2019-01-26T06:55:05.851Z
fiservlending.com	2019-01-26T06:55:04.783Z
fiserv.net	2019-01-26T06:55:04.681Z
fiservfsc.com	2019-01-26T06:55:04.598Z
summitsite.com	2019-01-26T06:55:04.573Z
fiservboston.com	2019-01-26T06:55:04.491Z
fiservcws.com	2019-01-26T06:55:04.033Z
fiservsa4.com	2019-01-26T06:54:28.430Z
fiservsw.com	2019-01-26T06:54:28.399Z
zashpayfromfiserv.info	2019-01-26T06:54:27.588Z
onefiserv.biz	2019-01-26T06:54:27.580Z
zashpaybyfiserv.info	2019-01-26T06:54:27.561Z
efiserv.com	2019-01-26T06:54:27.550Z
fiservip.net	2019-01-26T06:54:27.505Z
fiservsw.net	2019-01-26T06:54:27.473Z
onefiserv.us	2019-01-26T06:54:26.782Z
zashatfiserv.info	2019-01-26T06:54:05.841Z
fiservcsi.info	2019-01-26T06:54:05.645Z
zashpaybyfiserv.mobi	2019-01-26T06:54:04.494Z
fiservla4.com	2019-01-26T06:54:04.487Z
fiservpit.com	2019-01-26T06:54:04.409Z
zashpay-fiserv.info	2019-01-26T06:54:01.736Z
zashatfiserv.mobi	2019-01-26T06:54:00.108Z
fiservvpn.net	2019-01-26T06:50:18.585Z
zashatfiserv.biz	2019-01-26T06:50:18.584Z
fiservcpsclients.com	2019-01-26T06:50:18.532Z
fiservse.com	2019-01-26T06:50:18.429Z
fiservbusiness.com	2019-01-26T06:50:18.351Z

fiservapps.org	2019-01-26T06:50:17.036Z
fiservsupport.com	2019-01-26T06:50:16.952Z
fiservdm.net	2019-01-26T06:50:16.951Z
agiliti-fiserv.com	2019-01-26T06:50:16.951Z
fiservwebsolutions.com	2019-01-26T06:50:16.828Z
fiserverdc.com	2019-01-26T06:50:15.775Z
zashpayfromfiserv.mobi	2019-01-26T06:50:15.774Z
esolutionsfiserv.com	2019-01-26T06:50:15.632Z
fiservsa6.com	2019-01-26T06:50:15.632Z
zashpayfiserv.info	2019-01-26T06:49:04.697Z
fiservdmdr.net	2019-01-26T06:49:04.613Z
zashpayfiserv.net	2019-01-26T06:49:04.269Z
zashpayfiserv.biz	2019-01-26T06:49:04.235Z
zash-fiserv.info	2019-01-26T06:49:04.213Z
fiservdm.info	2019-01-26T06:49:04.020Z
zashpaybyfiserv.biz	2019-01-26T06:49:03.084Z
fiservcreditservices.com	2019-01-26T06:49:03.083Z
fiservsourceone.com	2019-01-26T06:49:03.025Z
fiservservices.org	2019-01-26T06:47:53.340Z
onefiserv.mobi	2019-01-26T06:47:51.179Z
fiservapps.com	2019-01-26T06:47:51.075Z
fiservdirectsource.com	2019-01-26T06:47:51.071Z
fiservsa91.com	2019-01-26T06:47:50.975Z
zashpayfiserv.mobi	2019-01-26T06:47:50.305Z
zashpay-fiserv.biz	2019-01-26T06:47:50.281Z
users.com	2019-01-26T06:47:39.414Z
fiservservices.com	2019-01-26T06:47:39.329Z
agility-fiserv.com	2019-01-26T06:47:39.245Z
fiservsa92.com	2019-01-26T06:47:39.230Z
zashpay-fiserv.mobi	2019-01-26T06:47:38.736Z
fiserv-europe.net	2019-01-26T06:46:45.411Z
zashatfiserv.org	2019-01-26T06:46:45.101Z

fiservinsurance.com	2019-01-26T06:46:44.901Z
fiservls.com	2019-01-26T06:46:42.804Z
zash-fiserv.org	2019-01-26T06:46:42.481Z
fiservoutputsolutions.com	2019-01-26T06:46:41.975Z
fiservatlanta.com	2019-01-26T06:46:41.825Z
mybills.com	2019-01-26T06:46:41.816Z
fiservipvpn.com	2019-01-26T06:46:41.814Z
fiservsa5.com	2019-01-26T06:46:41.800Z
fiservsa3.com	2019-01-26T06:46:41.757Z
zash-fiserv.mobi	2019-01-26T06:46:40.509Z
zash-fiserv.biz	2019-01-26T06:46:40.443Z
hepsiian.com	2019-01-26T06:46:40.344Z
fiservsa93.com	2019-01-26T06:46:40.315Z
zashpaybyfiserv.org	2019-01-26T06:46:38.041Z
fiservlos.com	2019-01-26T06:46:37.897Z
fiservrmd.com	2019-01-26T06:44:35.486Z
fiservip.com	2019-01-26T06:44:35.429Z
zashpayfromfiserv.biz	2019-01-26T06:44:35.396Z
zashpayfiserv.org	2019-01-26T06:44:35.309Z
carreker.com	2019-01-26T06:44:35.199Z
fiservsa1.com	2019-01-26T06:44:35.119Z
fiservlendingsolutions.com	2019-01-26T06:21:47.000Z
fiservlemans.com	2019-01-26T04:56:36.225Z
jeromegroup.com	2019-01-26T04:19:36.293Z
fiserv-galaxy.com	2019-01-26T04:16:50.785Z

Create a valid Sender Policy Framework (SPF) record. Ensure the configuration of the SPF DNS record to verify syntax and MTA servers. Test the configuration to make sure its valid by checking the header of an incoming email looking for "spf=pass" Allow for DNS caching during testing; it may take up to 48 hours to fully propagate across the Internet. The nature of the SMTP protocol does not allow for complete prevention of spoofed emails, however the SPF header will reveal whether the email is authentic.

ABOUT THIS ISSUE

The Sender Policy Framework (SPF) is a simple but effective email-validation technique designed to detect the forgery of email (also called email spoofing). An SPF record is a mechanism that allows a receiving email server to validate that inbound email from a particular domain comes from a server that is authorized to send email on behalf of that particular domain. The list of authorized sending hosts for a domain is published as a Domain Name System (DNS) record for that domain in the form of a specially formatted TXT record. An SPF record is required for spoofed e-mail prevention and anti-spam control.

DNS HEALTH > ISSUE DETAIL

SPF Record Contains a Softfail

Softfail attributes in SPF makes spoofing and phishing email possible.

-1.6 SCORE IMPACT

5 findings

DOMAIN	RECORD	ANALYSIS	LAST SEEN
checkfree.com	v=spf1 a:mailout.checkfree.com a:outbd-pstfx.customercenter.net a:mail.apsnet.com a:mail2.checkfree.com a:mail09.rm04.net a:mailout- oh.checkfree.com a:outbd-pstfx- oh.customercenter.net ip4:204.95.150.228 ip4:12.145.177.240 ~all		2019-01-30T15:37:27.046Z
pcsbanking.com	-	-	2019-01-26T06:55:04.783Z
fiservatlanta.net	v=spf1 a mx ~all	-	2019-01-26T06:54:27.643Z
fiserv.com	v=spf1 include:_spf1.fiserv.com include:_spf2.fiserv.com include:_spf3.fiserv.com [~] all	-	2019-01-26T06:47:53.557Z
fiserv-ecomhosting.com	v=spf1 ip4:166.73.19.0/24 ip4:12.145.177.0/24 ip4:12.16.164.60 ip4:204.95.150.32 a mx a:phantom.cusa.com ~all	-	2019-01-08T22:31:57.833Z

To resolve this issue, enumerate the list of email servers that are authorized to send email on behalf of the domain. Update the SPF record with the correct email authorization list.

ABOUT THIS ISSUE

The Sender Policy Framework (SPF) is a simple but effective email-validation technique designed to detect the forgery of email (also called email spoofing). An SPF record is a mechanism that allows a receiving email server to validate that inbound email from a particular domain comes from a server that is authorized to send email on behalf of that particular domain. The list of authorized sending hosts for a domain is published as a Domain Name System (DNS) record for that domain in the form of a specially formatted TXT record. An SPF record is required for spoofed e-mail prevention and anti-spam control. However, if a softfail attribute is included, it is still possible to spoof email from a particular domain. An SPF record has been detected for the domain.



PATCHING CADENCE

ISSUE COUNT

ABOUT THIS FACTOR

The table below includes a list of issues searched for and indicates which issues were found.

The Patching Cadence module analyzes how quickly a company reacts to vulnerabilities to measure patching practices. We look at the rate at which it takes a company to remediate and apply patches compared to peers.



PATCHING CADENCE > ISSUE DETAIL

High-Severity Vulnerability in Last Observation

We observed a high-severity vulnerability during our last scan, which may still be publicly exposed.

-0.4 SCORE

5 findings

ID	URL	PUBLICATION DATE	DESTINATION IP	DESTINATION PORT	LAST SEEN
CVE-2017-9078	https://nvd.nist.gov/vu In/detail/CVE-2017- 9078	2017-05-19	65.206.30.72	22	2019-01- 09T11:33:16.785Z
Description: The server in Dropbear be TCP listeners when the -a	efore 2017.75 might allow post option is enabled.	-authentication root remote o	code execution because of a o	double free in cleanup of	
CVE-2016-2776	https://nvd.nist.gov/vu In/detail/CVE-2016- 2776	2016-09-28	64.149.172.30	53	2019-01- 01T15:31:06.385Z
	IND 9 before 9.9.9-P3, 9.10.x t kers to cause a denial of servi			erly construct responses,	
CVE-2015-5477	https://nvd.nist.gov/vu In/detail/CVE-2015- 5477	2015-07-29	64.149.172.30	53	2019-01- 01T15:31:06.385Z
Description: named in ISC BIND 9.x be failure and daemon exit) v	fore 9.9.7-P2 and 9.10.x before a TKEY queries.	e 9.10.2-P3 allows remote att	ackers to cause a denial of se	ervice (REQUIRE assertion	
CVE-2014-8500	https://nvd.nist.gov/vu In/detail/CVE-2014-	2014-10-12	64.149.172.30	53	2019-01- 01T15:31:06.385Z

	8500				
	n 9.8.x, 9.9.0 through 9.9.6, and 9 rvice (memory consumption and r				e attackers
CVE-2015-5722	https://nvd.nist.gov/vu In/detail/CVE-2015- 5722	2015-09-04	64.149.172.30	53	2019-01- 01T15:31:06.385Z
Description: buffer.c in named in ISC BIND 9.x before 9.9.7-P3 and 9.10.x before 9.10.2-P4 allows remote attackers to cause a denial of service (assertion failure and daemon exit) by creating a zone containing a malformed DNSSEC key and issuing a query for a name in that zone.					

Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment. Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the Bugtraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular update schedule for all software and hardware in use within your organization, ensuring that all the latest patches are applied soon after they are released.

ABOUT THIS ISSUE

Common vulnerabilities and exposures (CVE) is a list of publicly-known vulnerabilities in software and hardware. Each CVE contains an ID, a description of the vulnerability, and the product names and versions which are affected by the vulnerability. Software and hardware frequently self-report their product name and version when hosts connect to them. By searching through the CVE list and cross-referencing the names and versions of products found on this company's network, we are able to infer the presence of vulnerabilities.

PATCHING CADENCE > ISSUE DETAIL

High Severity CVEs Patching Cadence

High severity vulnerability seen on network more than 30 days after CVE was published.

-0.9 SCORE

41 findings

ID	URL	PUBLICATION DATE	DESTINATION IP	DESTINATION PORT	LAST SEEN	
CVE-2014-3515	https://nvd.nist.gov/vu In/detail/CVE-2014- 3515	2014-07-09	209.163.213.134	443	2018-12- 16T13:13:28.000Z	
type after unserialization, v	IP before 5.4.30 and 5.5.x before stackers allows remote attackers a confusion" issues in (1) Arrayo	to execute arbitrary code via	a crafted string that triggers			
CVE-2014-9427	https://nvd.nist.gov/vu In/detail/CVE-2014- 9427	2015-01-02	209.163.213.134	443	2018-12- 16T13:13:28.000Z	
.php file, does not properly newline character, which c	CGI component in PHP throug y consider the mapping's leng causes an out-of-bounds read aging the ability to upload a .pl it to the mapping.	th during processing of an inv and might (1) allow remote att	valid file that begins with a # of tackers to obtain sensitive info	character and lacks a prmation from php-cgi		
CVE-2014-3669	https://nvd.nist.gov/vu In/detail/CVE-2014- 3669	2014-10-29	209.163.213.134	443	2018-12- 16T13:13:28.000Z	
Description: Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the						

Indexaption: This SPL component in P-IP before 5.430 and 5.6 x bidder 5.534 incorectly anticipates that cartain data structures will have the army data growth programment of the progra	unserialize function that tr	riggers calculation of a large le	nath value			
Inidetail/CVE-2014-3515 Description: This SR. Company or in PIP before 5.530 and 5.6 x before 5.54 hearizestly intelligens that cartain data structures will have the array data distinction relationship to the company of the compan	and an arrange function that the	.ggs.5 calculation of a large le	g value.			
The SPIC components in PHP before 6.3.03 and 5.3.5 before 5.5.4 in controctly anticipients take certain data structures with have the array data year after unsertaintain, which a latuse remote state.tents to security with a critical darking that triggers are of a Hashinable interaction, related to type confision in source of a Hashinable interaction, related to type confision in the confision of source in 10 American and 10 Am	CVE-2014-3515	In/detail/CVE-2014-	2014-07-09	209.163.213.134	80	
Description: Integer overflow in the object custom function in existanciard/var_unserializer. In PHP before 5.4.34, 5.5x before 5.5.18, and 5.6x before 5.62 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserializer function that fugiese calculation of a large length value. CVE-2014-9427	The SPL component in PH type after unserialization,	which allows remote attackers	to execute arbitrary code via	a a crafted string that triggers		
Integer overflow in the object_custom function in exists-induction and exists-induction of a large length value. CVE-2014-9427	CVE-2014-3669	In/detail/CVE-2014-	2014-10-29	209.163.213.134	80	
In/detail/CVE-2014-9427 Description: spike(pigle_main.c in the Coli component in PHP through 5.4.36, 5.5x through 5.5.20, and 5.6x through 5.6.4, when mmap is used to read a phop file, does not properly consider the mapping's length during processing of an invalid file that begins with a 2 character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a _php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping. CVE-2014-9427 https://mvd.nist.gov/vu 2015-01-02 12.14.174.237 - 2018-06-0713:25.54.0002 Pescription: applicative consider the mapping is length during processing of an invalid file that begins with a 2 character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a _php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping. CVE-2014-9427 https://mvd.nist.gov/vu 2015-01-02 12.14.174.237 - 2018-05-1913:05:22.0002 Pescription: a physical control of the mapping is length during processing of an invalid file that begins with a 2 character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a _php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations and properly consider the mapping is length during processing of an invalid file that begins with a 2 character and lacks a newline character, which causes an out-of-bounds read and rain might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to publical a php file	5.6.2 allows remote attack	kers to cause a denial of servic	e (application crash) or possi			
spal/cigicg_main in the CGI component in PHP through 5.4.36, 5.5x through 5.5.20, and 5.6 x through 5.6.4, when mmap is used to read a phypific file, does not properly consider the mappings is englished the property consider the mappings is englished the property consider the mappings. CVE-2014-9427 https://nvd.nist.gov/vu_9427 Description: application to the CGI component in PHP through 5.4.36, 5.5x through 5.5.20, and 5.6x through 5.6.4, when mmap is used to read a phypific or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping. CVE-2014-9427 https://nvd.nist.gov/vu_9427 Description: application to the CGI component in PHP through 5.4.36, 5.5x through 5.5.20, and 5.6x through 5.6.4, when mmap is used to read a phypific or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping. CVE-2014-9427 https://nvd.nist.gov/vu_19427 Description: application to the CGI component in PHP through 5.4.36, 5.5x through 5.5.20, and 5.6x through 5.6.4, when mmap is used to read a phypific or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping. CVE-2014-9427 https://nvd.nist.gov/vu_19427 Description: application to the CGI component in PHP through 5.4.36, 5.5x through 5.5.20, and 5.6x through 5.6.4, when mmap is used to read a phypific or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping. CVE-2014-9427 https://nvd.nist.gov/vu_19427 Description: application to the CGI component in PHP through 5.4.36, 5.5x through 5.5.20, and 5.6x through 5.6.4, when mmap is used to read a phypific or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping. CVE-2018-6789 https://nvd.nist.gov/vu_19428 Description: An issue was discovered in the base64d function in the SMTP disense in Exim before 4.90.1. By sending a handcrafted	CVE-2014-9427	In/detail/CVE-2014-	2015-01-02	209.163.213.134	80	
In/detail/CVE-2014-9427 Description: sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (il) allow remote tattackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping. CVE-2014-9427 https://mvd.nist.gov/vu 2015-01-02 12.14.174.237 - 2018-05- 1p/10detail/CVE-2014- 9427 Pescription: sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (il) allow remote tattackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping. CVE-2018-6789 https://mvd.nist.gov/vu 2018-02-08 2018-02-08 209.221.136.222 2018-04- 20172:00.15.0002 Description: An issue was discovered in the base64d function in the SMTP listener in Exim before 4.90.1. By sending a handcrafted message, a buffer overflow may happen. This can be used to execute code remotely. CVE-2017-16943 https://mvd.nist.gov/vu 2017-11-25 2018-04- 20172:00.15.0002 Description: The receive_msg function in receive.c in the SMTP daemon in Exim 4.88 and 4.89 allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via vectors involving BDAT commands. CVE-2017-3167 https://nvd.nist.gov/vu 2017-06-19 19708:01-30.0002	.php file, does not properl newline character, which process memory by levera	ly consider the mapping's leng causes an out-of-bounds read aging the ability to upload a .pl	th during processing of an inv and might (1) allow remote att	valid file that begins with a # o tackers to obtain sensitive info	character and lacks a ormation from php-cgi	
sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.4.20, and 5.6.x through 5.6.4. When mmap is used to read a phph file, does not propely consider the mapping's length during processing of an invall file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (f) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping. CVE-2014-9427	CVE-2014-9427	In/detail/CVE-2014-	2015-01-02	12.14.174.237	-	
In/detail/CVE-2014-9427 Description: sapi/cgl/Cgl_mainc. in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a phyph file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (f) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping. CVE-2018-6789 https://nvd.nist.gov/vu ln/detail/CVE-2018-6789 Description: An issue was discovered in the base64d function in the SMTP listener in Exim before 4.90.1. By sending a handcrafted message, a buffer overflow may happen. This can be used to execute code remotely. CVE-2017-16943 https://nvd.nist.gov/vu ln/detail/CVE-2017-16943 https://nvd.nist.gov/vu ln/detail/CVE-2017-16943 Description: The receive_msg function in receive.c in the SMTP daemon in Exim 4.88 and 4.89 allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via vectors involving BDAT commands. CVE-2017-3167 https://nvd.nist.gov/vu ln/detail/CVE-2017-1708-019 198.167.0.48 - 2018-04-19108:013.0.000Z	php file, does not properl newline character, which process memory by levera	ly consider the mapping's leng causes an out-of-bounds read aging the ability to upload a .pl	th during processing of an invaled and might (1) allow remote att	valid file that begins with a # o tackers to obtain sensitive info	character and lacks a ormation from php-cgi	
sapicgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5 x. through 5.5.20, and 5.6 x. through 5.6.4, when mmap is used to read a php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (f) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping. CVE-2018-6789 https://nvd.nist.gov/vu	CVE-2014-9427	In/detail/CVE-2014-	2015-01-02	12.14.174.237	-	
In/detail/CVE-2018-6789 Description: An issue was discovered in the base64d function in the SMTP listener in Exim before 4.90.1. By sending a handcrafted message, a buffer overflow may happen. This can be used to execute code remotely. CVE-2017-16943 https://nvd.nist.gov/vu ln/detail/CVE-2017-16943 https://nvd.nist.gov/vu ln/detail/CVE-2017-16943 Description: The receive_msg function in receive.c in the SMTP daemon in Exim 4.88 and 4.89 allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via vectors involving BDAT commands. CVE-2017-3167 https://nvd.nist.gov/vu ln/detail/CVE-2017- In/detail/CVE-2017- 198.167.0.48 - 2018-04- 19T08:01:30.000Z	.php file, does not properl newline character, which process memory by levera	ly consider the mapping's leng causes an out-of-bounds read aging the ability to upload a .pl	th during processing of an inv and might (1) allow remote att	valid file that begins with a # o tackers to obtain sensitive info	character and lacks a ormation from php-cgi	
An issue was discovered in the base64d function in the SMTP listener in Exim before 4.90.1. By sending a handcrafted message, a buffer overflow may happen. This can be used to execute code remotely. CVE-2017-16943	CVE-2018-6789	In/detail/CVE-2018-	2018-02-08	209.221.136.222	-	
In/detail/CVE-2017- 16943 Description: The receive_msg function in receive.c in the SMTP daemon in Exim 4.88 and 4.89 allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via vectors involving BDAT commands. CVE-2017-3167 https://nvd.nist.gov/vu 2017-06-19 198.167.0.48 - 2018-04-In/detail/CVE-2017- 19T08:01:30.000Z				4.90.1. By sending a handcra	fted message, a buffer	
The receive_msg function in receive.c in the SMTP daemon in Exim 4.88 and 4.89 allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via vectors involving BDAT commands. CVE-2017-3167 https://nvd.nist.gov/vu 2017-06-19 198.167.0.48 - 2018-04-In/detail/CVE-2017- 19T08:01:30.000Z	CVE-2017-16943	In/detail/CVE-2017-	2017-11-25	209.221.136.222	-	
In/detail/CVE-2017- 19T08:01:30.000Z				ows remote attackers to exec	ute arbitrary code or cause	
	CVE-2017-3167	In/detail/CVE-2017-	2017-06-19	198.167.0.48	-	

	fore 2.2.33 and 2.4.x before 2.4 y lead to authentication require		_auth_pw() by third-party mo	dules outside of the	
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	198.167.0.17	-	2018-04- 19T08:01:30.000Z
	fore 2.2.33 and 2.4.x before 2.4 y lead to authentication require		_auth_pw() by third-party mo	dules outside of the	
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	208.11.141.204	-	2018-04- 19T04:28:41.000Z
	fore 2.2.33 and 2.4.x before 2.4 y lead to authentication require		_auth_pw() by third-party mo	dules outside of the	
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	208.11.141.167	-	2018-04- 19T04:28:41.000Z
	fore 2.2.33 and 2.4.x before 2.4 y lead to authentication require		_auth_pw() by third-party mo	dules outside of the	
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	208.11.141.196	-	2018-04- 19T04:28:41.000Z
	fore 2.2.33 and 2.4.x before 2.4 y lead to authentication require		_auth_pw() by third-party mo	dules outside of the	
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	208.11.141.177	-	2018-04- 19T04:28:41.000Z
	fore 2.2.33 and 2.4.x before 2.4 y lead to authentication require		_auth_pw() by third-party mo	dules outside of the	
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	208.11.141.192	-	2018-04- 19T04:28:41.000Z
	fore 2.2.33 and 2.4.x before 2.4 y lead to authentication require		_auth_pw() by third-party mo	dules outside of the	
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	192.131.55.82	-	2018-04- 19T04:28:41.000Z
	fore 2.2.33 and 2.4.x before 2.4 y lead to authentication require		_auth_pw() by third-party mo	dules outside of the	
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	208.11.141.91	-	2018-04- 19T04:28:41.000Z
	fore 2.2.33 and 2.4.x before 2.4 y lead to authentication require		_auth_pw() by third-party mo	dules outside of the	
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017-	2017-06-19	208.11.141.155	-	2018-04- 19T04:28:41.000Z

	3167				
	re 2.2.33 and 2.4.x before 2.4 lead to authentication require		_auth_pw() by third-party mod	dules outside of the	
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	208.11.141.88	-	2018-04- 19T04:28:41.000Z
	re 2.2.33 and 2.4.x before 2.4 lead to authentication require		_auth_pw() by third-party mod	dules outside of the	
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	192.131.72.203	-	2018-04- 19T04:28:41.000Z
	re 2.2.33 and 2.4.x before 2.4 lead to authentication require		_auth_pw() by third-party mod	dules outside of the	
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	208.11.141.73	-	2018-04- 19T04:28:41.000Z
	re 2.2.33 and 2.4.x before 2.4 lead to authentication require		_auth_pw() by third-party mod	dules outside of the	
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	208.11.141.78	-	2018-04- 19T04:28:41.000Z
	re 2.2.33 and 2.4.x before 2.4 lead to authentication require		_auth_pw() by third-party mod	dules outside of the	
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	192.131.55.83	-	2018-04- 19T04:28:41.000Z
	re 2.2.33 and 2.4.x before 2.4 lead to authentication require		_auth_pw() by third-party mod	dules outside of the	
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	208.11.141.75	-	2018-04- 19T04:28:41.000Z
	re 2.2.33 and 2.4.x before 2.4 lead to authentication require		_auth_pw() by third-party mod	dules outside of the	
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	208.11.141.64	-	2018-04- 19T04:28:41.000Z
	re 2.2.33 and 2.4.x before 2.4 lead to authentication require		_auth_pw() by third-party mod	dules outside of the	
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	208.11.141.132	-	2018-04- 19T04:28:41.000Z
	re 2.2.33 and 2.4.x before 2.4 lead to authentication require		_auth_pw() by third-party mod	dules outside of the	

CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	64.128.99.203	-	2018-04- 19T02:12:57.000Z		
	ore 2.2.33 and 2.4.x before 2.4 rlead to authentication require		_auth_pw() by third-party mod	dules outside of the			
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	198.167.0.33	-	2018-04- 19T01:35:31.000Z		
	ore 2.2.33 and 2.4.x before 2.4 lead to authentication require		_auth_pw() by third-party mod	dules outside of the			
CVE-2017-3167	https://nvd.nist.gov/vu ln/detail/CVE-2017- 3167	2017-06-19	198.167.0.248	-	2018-04- 19T01:35:31.000Z		
	ore 2.2.33 and 2.4.x before 2.4 I lead to authentication require		_auth_pw() by third-party mod	dules outside of the			
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	63.240.88.6	-	2018-04- 19T01:35:31.000Z		
	ore 2.2.33 and 2.4.x before 2.4 lead to authentication require		_auth_pw() by third-party mod	dules outside of the			
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	198.167.0.148	-	2018-04- 19T01:35:31.000Z		
	ore 2.2.33 and 2.4.x before 2.4 I lead to authentication require		_auth_pw() by third-party mod	dules outside of the			
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	198.167.0.246	-	2018-04- 19T01:35:31.000Z		
	ore 2.2.33 and 2.4.x before 2.4 I lead to authentication require		_auth_pw() by third-party mod	dules outside of the			
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	166.73.6.118	-	2018-04- 19T01:35:31.000Z		
	ore 2.2.33 and 2.4.x before 2.4 I lead to authentication require		_auth_pw() by third-party mod	dules outside of the			
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	198.167.0.133	-	2018-04- 19T01:35:31.000Z		
	Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.						
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	64.149.172.15	-	2018-04- 17T12:50:05.000Z		
Description: In Apache httpd 2.2.x bef	ore 2.2.33 and 2.4.x before 2.4	1.26, use of the ap_get_basic	_auth_pw() by third-party mod	dules outside of the			

authentication phase may lead to authentication requirements being bypassed.						
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	64.149.172.137 -	2018-04- 17T12:50:05.000Z		
	fore 2.2.33 and 2.4.x before 2.4 y lead to authentication require		:_auth_pw() by third-party modules outside of the			
CVE-2017-3167	https://nvd.nist.gov/vu In/detail/CVE-2017- 3167	2017-06-19	209.163.213.134 -	2018-04- 12T19:04:32.000Z		
	fore 2.2.33 and 2.4.x before 2.4 y lead to authentication require		:_auth_pw() by third-party modules outside of the			
CVE-2014-3669	https://nvd.nist.gov/vu In/detail/CVE-2014- 3669	2014-10-29	209.163.213.134 -	2018-04- 12T19:04:32.000Z		
5.6.2 allows remote attack	Description: Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.					
CVE-2014-3515	https://nvd.nist.gov/vu In/detail/CVE-2014- 3515	2014-07-09	209.163.213.134 -	2018-04- 12T19:04:32.000Z		
Description:						

Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the BugTraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.

destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.

ABOUT THIS ISSUE

Based on scan data, the company had high severity CVE vulnerability that was open longer than 30 days after the CVE was published. High severity CVEs are those with a documented CVSS severity over 7.0. It is best practice in standards such as PCI DSS to mitigate or patch high severity vulnerabilities within 30 days. Details on each vulnerability are listed in the table below.

PATCHING CADENCE > ISSUE DETAIL

Medium-Severity Vulnerability in Last Observation

We observed a medium-severity vulnerability during our last scan, which may still be publicly exposed.

The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable

-0.6 SCORE

382 findings

ID	URL	PUBLICATION DATE	DESTINATION IP	DESTINATION PORT	LAST SEEN
CVE-2017-3736	https://nvd.nist.gov/vu In/detail/CVE-2017- 3736	2017-11-02	208.11.141.91	443	2019-01- 18T07:44:06.000Z
Description:					

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.11.141.91 443 2019-01-

In/detail/CVE-2017-

3738

18T07:44:06.000Z

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.91 2019-01-443

In/detail/CVE-2015-

3185

18T07:44:06.000Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.91 443 2019-01-

In/detail/CVE-2014-

0226

18T07:44:06.000Z

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.91 2019-01-443

In/detail/CVE-2016-

8743

18T07:44:06.000Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208 11 141 91 443 2019-01-

In/detail/CVE-2015-

3183

3737

18T07:44:06.000Z

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 208.11.141.91 443 2019-01-

In/detail/CVE-2017-

18T07:44:06.000Z

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2015-3185 https://nvd.nist.gov/vu 198.246.154.102 2015-07-20 443 2019-01-In/detail/CVE-2015-18T04:30:46.000Z 3185 Description: The an_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior. CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 198.246.154.102 443 2019-01-In/detail/CVE-2017-18T04:30:46.000Z 3738 Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository. CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 198.246.154.102 443 2019-01-In/detail/CVE-2015-18T04:30:46.000Z 3183 Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c. https://nvd.nist.gov/vu CVE-2014-0226 2019-01-2014-07-20 198 246 154 102 443 In/detail/CVE-2014-18T04:30:46.000Z 0226 Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c. CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 198.246.154.102 443 2019-01-In/detail/CVE-2017-18T04:30:46.000Z 3737 Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected. CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 198.246.154.102 443 2019-01-In/detail/CVE-2016-18T04:30:46.000Z 8743 Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution. CVE-2017-3736 2017-11-02 https://nvd.nist.gov/vu 198.246.154.102 443 2019-01-In/detail/CVE-2017-18T04:30:46.000Z 3736 Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC

algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 198.167.0.246 443 2019-01-

In/detail/CVE-2016-17T22:12:01.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 443 192.131.76.193 2019-01-

In/detail/CVE-2015-

3183

17T20:37:00.000Z

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 192.131.76.193 443 2019-01-

In/detail/CVE-2014-

0226

17T20:37:00.000Z

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 192.131.76.193 443 2019-01-

In/detail/CVE-2017-

3737

17T20:37:00.000Z

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

2017-12-07 CVE-2017-3738 https://nvd.nist.gov/vu 192.131.76.193 443 2019-01-

In/detail/CVE-2017-

3738

17T20:37:00.000Z

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0q are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository,

CVE-2015-3185 https://nvd.nist.gov/vu 2019-01-2015-07-20 192.131.76.193 443

In/detail/CVE-2015-

3185

17T20:37:00.000Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 192 131 76 193 2019-01-443 In/detail/CVE-2017-17T20:37:00.000Z Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen. 2017-07-27 CVE-2016-8743 https://nvd.nist.gov/vu 192.131.76.193 443 2019-01-In/detail/CVE-2016-17T20:37:00.000Z 8743 Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution. CVE-2017-5647 https://nvd.nist.gov/vu 2017-04-17 208.74.12.10 443 2019-01-In/detail/CVE-2017-17T17:11:34.000Z 5647 Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C. CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 198.167.0.148 443 2019-01-In/detail/CVE-2016-17T16:00:30.000Z 8743 Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution. CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 166.73.14.52 443 2019-01-In/detail/CVE-2017-17T14:47:18.000Z 3737 Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not as designed to the explicit hardsake full-close (SSL_Co_Introduce), SSL_despty and SSL_Control (SSL_read) or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected. CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 166.73.14.52 443 2019-01-In/detail/CVE-2017-17T14:47:18.000Z 3738 Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository. CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 166.73.14.52 443 2019-01-

	In/detail/CVE-2014- 0226				17T14:47:18.000Z
(heap-based buffer overfl	d_status module in the Apache ow), or possibly obtain sensitive dling within the status_handler	e credential information or ex	ecute arbitrary code, via a cra	afted request that triggers	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	166.73.14.52	443	2019-01- 17T14:47:18.000Z
lines and headers. Accep	all releases prior to 2.2.32 and 2 ting these different behaviors r pplication servers, either throug tting and cache pollution.	epresented a security conce	rn when httpd participates in a	any chain of proxies or	
CVE-2017-3736	https://nvd.nist.gov/vu In/detail/CVE-2017- 3736	2017-11-02	166.73.14.52	443	2019-01- 17T14:47:18.000Z
algorithms are affected. A are not believed likely. At information about a privat likely only accessible to a target private key in a sce	ing bug in the x86_64 Montgor Analysis suggests that attacks a tacks against DH are considere te key may be performed offline I limited number of attackers. Al enario with persistent DH param the BMI1, BMI2 and ADX extensi	gainst RSA and DSA as a res ed just feasible (although very e. The amount of resources r n attacker would additionally neters and a private key that	ult of this defect would be ver difficult) because most of the equired for such an attack wo need online access to an unp is shared between multiple cli	y difficult to perform and e work necessary to deduce uld be very significant and patched system using the ients. This only affects	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	166.73.14.52	443	2019-01- 17T14:47:18.000Z
remote attackers to cond	ding implementation in the Apac uct HTTP request smuggling at haracters in modules/http/http_	tacks via a crafted request, re			
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	166.73.14.52	443	2019-01- 17T14:47:18.000Z
directive may be associat	rired function in server/request. Led with an authorization setting ons in opportunistic circumstand	rather than an authenticatio	n setting, which allows remote	e attackers to bypass	
CVE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	166.73.14.117	443	2019-01- 17T14:47:17.000Z
handshake then OpenSSI as designed for the explicit work correctly if SSL_rear initial function call. If SSL_is passed without being dhave to be present that re	om version 1.0.2b) introduced at L would move into the error static handshake functions (SSL_dd) or SSL_write() is called directread()/SSL_write() is subsequelecrypted/encrypted directly frosulted in a call to SSL_read()/St. Fixed in OpenSSL 1.0.2n. Opens	te and would immediately fai o_handshake(), SSL_accept() tly. In that scenario, if the har ntly called by the application im the SSL/TLS record layer. SL_write() being issued after	I if you attempted to continue and SSL_connect()), howeven dshake fails then a fatal error for the same SSL object then In order to exploit this issue a	the handshake. This works r due to a bug it does not will be returned in the it will succeed and the data n application bug would	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	166.73.14.117	443	2019-01- 17T14:47:17.000Z
lines and headers. Accep	all releases prior to 2.2.32 and 2 ting these different behaviors r pplication servers, either throug tting and cache pollution.	epresented a security conce	rn when httpd participates in a	any chain of proxies or	

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 166.73.14.117 443 2019-01-In/detail/CVE-2017-17T14:47:17.000Z 3738 Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository. CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 166.73.14.117 443 2019-01-In/detail/CVE-2015-17T14:47:17.000Z 3185 Description: The an_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior. CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 166.73.14.117 443 2019-01-17T14:47:17.000Z In/detail/CVE-2014-0226 Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c. CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 166.73.14.117 443 2019-01-17T14:47:17.000Z In/detail/CVE-2017-3736 Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen. CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 166.73.14.117 443 2019-01-In/detail/CVE-2015-17T14:47:17.000Z 3183 The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c. 2017-07-27 CVE-2016-8743 https://nvd.nist.gov/vu 443 2019-01-166.73.13.244 In/detail/CVE-2016-17T14:40:11.000Z 8743 Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution. CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 443 2019-01-166 73 13 244 In/detail/CVE-2017-17T14:40:11.000Z 3737 Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a

handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2015-3185	https://nvd.nist.gov/vu	2015-07-20	166.73.13.244	443	2019-01-
	In/detail/CVE-2015-				17T14:40:11.000Z
	3185				

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2014-0226	https://nvd.nist.gov/vu	2014-07-20	166.73.13.244	443	2019-01-
	In/detail/CVE-2014-				17T14:40:11.000Z
	0226				

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3738	https://nvd.nist.gov/vu	2017-12-07	166.73.13.244	443	2019-01-
	In/detail/CVE-2017-				17T14:40:11.000Z
	3738				

Description

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2015-3183	https://nvd.nist.gov/vu	2015-07-20	166.73.13.244	443	2019-01-
	In/detail/CVE-2015-				17T14:40:11.000Z
	3183				

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2017-3736	https://nvd.nist.gov/vu	2017-11-02	166.73.13.244	443	2019-01-
	In/detail/CVE-2017-				17T14:40:11.000Z
	3736				

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	198.167.0.33	443	2019-01- 17T12:44:23.000Z
---------------	--	------------	--------------	-----	------------------------------

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

Lipse/Invedical/CVE-2015-3185 https://mvd.nist.gov/vu 2015-07-20 208.11.141.177 443 2019-01-17T10.54.06.0002 3185 Description: The sp. some_auth_required function in server/request_c in the Apache HTTP Server 24.x before 2.414 does not consider that a Require directive may be associated with an authorization setting rather than an authorization setting, which allows renote struckers to bypass intended access cere relatifications on porturnistic crumamostres by leveraging the presence of a module that relies on the 22.2 API behavior. CVE-2016-8743 https://mvd.nist.gov/vu 2017-07-27 208.11.141.177 443 2019-01-17T10.54.06.0002 Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-and application servers, when the proximal proxima
The ap. some_suth_required function in server/request. in the Apache HTTP Server 24.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting insert than an authorization setting insert before 2.4.14 does not properly passe intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior. CVE-2016-8743 https://mvd.nist.gov/vu 2017-07-27 208.11.141.177 443 2019-01-17110:54.06.0002 8743 Description: Apache HTTP Server in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpp apriticipates in any chain of proxies or interacts with backen dapplication servers, either through mod_proxy or using conventional CG mechanisms, and may result in request smuggling, response splitting and cache pollution. CVE-2015-3183 https://nvd.nist.gov/vu ln/detail/CVE-2015-3183 Description: The churked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invaled churk-extension characters in module-shiptinghtp. Diless. C. CVE-2017-3736 https://nvd.nist.gov/vu proxy or using procedure in OpenSE, before 1.0.2m and 1.10 before 1.1.0g. No EC approximation about a private key in a scenario characters or module-shiptinghtp. Diless. C. CVE-2017-3736 https://nvd.nist.gov/vu proxy p
Description: Apach e HTTP Server, in all treases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response sentences. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or inferences with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution. CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.11.41.177 443 2019-01-17710.54.06.000Z Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/hightb_filesrs. CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.11.141.177 443 2019-01-17710.54.06.000Z Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 10.2m and 11.0 before 11.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered ust feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be system using the target pane by no secretion of attackers. An attacker would additionally need online access to an unpacticed system using the target pane by no secretion of attackers. An attacker would additionally need online access to an unpacticed system using the target pane by no secretion of a such an attack would be required for such mattack would be system using the target pane by no secretion of the modules of the province of the work necessary to deduce information about a private k
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in an article of proxise or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache politicus. CVE-2015-3183
In/detail/CVE-2015-3183 Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http://fitp.fiters.c. CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.11.141.177 443 2019-01-117/10.54.06.000Z 3736 Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 10.2m and 1.10 before 11.0g, No EC algorithms are effected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persisten DH parameters and a private key that is shared between multiple-clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen. CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.177 443 2019-01-17710-54:06.000Z Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request. CVE-2017-3737 https://nvd.nist.gov/vu 2017-1
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct. HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c. CVE-2017-3736
In/detail/CVE-2017-3736 Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 11.0 before 1.1.0g, No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen. CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.177 443 2019-01-17T10:54:06.000Z 0226 Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c. CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 208.11.141.177 443 2019-01-17T10:54:06.000Z 3737 Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a
There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 11.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen. CVE-2014-0226
In/detail/CVE-2014- 0226 Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c. CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 208.11.141.177 443 2019-01-17T10:54:06.000Z 3737 Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c. CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 208.11.141.177 443 2019-01-17T10:54:06.000Z 3737 Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a
In/detail/CVE-2017- 3737 Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a
as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.
CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.11.141.177 443 2019-01- In/detail/CVE-2017- 3738 17T10:54:06.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a

private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.78 443 2019-01-In/detail/CVE-2014-17T10:51:31.000Z 0226

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.11.141.78 443 2019-01-

In/detail/CVE-2017-

3738

17T10:51:31.000Z

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.11.141.78 443 2019-01-In/detail/CVE-2017-17T10:51:31.000Z

3736

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.78 2019-01-443

In/detail/CVE-2016-

8743

17T10:51:31.000Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.78 443 2019-01-

In/detail/CVE-2015-

3185

17T10:51:31.000Z

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

https://nvd.nist.gov/vu 2017-12-07 CVE-2017-3737 208.11.141.78 443 2019-01-In/detail/CVE-2017-17T10:51:31.000Z

3737

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would

have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVF-2015-3183

https://nvd.nist.gov/vu In/detail/CVE-2015-

2015-07-20

208 11 141 78

443

2019-01-17T10:51:31.000Z

3183

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2016-8743

https://nvd.nist.gov/vu In/detail/CVE-2016-

2017-07-27 208.11.141.132 443

2019-01-17T10:50:47.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2017-3737

https://nvd.nist.gov/vu In/detail/CVE-20172017-12-07

208.11.141.132

208.11.141.132

443

2019-01-

17T10:50:47.000Z

3737

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being day of the same service. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2017-3738

https://nvd.nist.gov/vu In/detail/CVE-20172017-12-07

443

2019-01-

17T10:50:47.000Z

3738

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2017-3736

https://nvd.nist.gov/vu In/detail/CVE-20172017-11-02

208.11.141.132

443

2019-01-

17T10:50:47.000Z

3736

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2014-0226

https://nvd.nist.gov/vu In/detail/CVE-2014-

0226

2014-07-20

208.11.141.132

443

2019-01-

17T10:50:47.000Z

Description:

Race condition in the mod status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	208.11.141.132	443	2019-01- 17T10:50:47.000Z	
remote attackers to condu	ing implementation in the Apa act HTTP request smuggling at aracters in modules/http/http.	ttacks via a crafted request, re				
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	208.11.141.132	443	2019-01- 17T10:50:47.000Z	
directive may be associate	red function in server/request. ed with an authorization settin ns in opportunistic circumstan	g rather than an authenticatio	n setting, which allows remote	e attackers to bypass		
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	208.11.141.76	443	2019-01- 17T10:42:47.000Z	
remote attackers to condu	ing implementation in the Apa ict HTTP request smuggling at naracters in modules/http/http.	ttacks via a crafted request, re				
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	208.11.141.76	443	2019-01- 17T10:42:47.000Z	
(heap-based buffer overflo	_status module in the Apache ow), or possibly obtain sensitiv dling within the status_handler a_request.c.	e credential information or ex	ecute arbitrary code, via a cra	afted request that triggers		
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	208.11.141.76	443	2019-01- 17T10:42:47.000Z	
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.						
CVE-2017-3738	https://nvd.nist.gov/vu In/detail/CVE-2017- 3738	2017-12-07	208.11.141.76	443	2019-01- 17T10:42:47.000Z	
are affected. Analysis suggested likely. Attacks ag private key may be perforn TLS to be meaningful, the 2016-0701. This only affect from this issue is similar to Fixed in OpenSSL 1.0.2n. I.	n the AVX2 Montgomery mult gests that attacks against RSA ainst DH1024 are considered med offline. The amount of res server would have to share th ts processors that support the CVE-2017-3736, CVE-2017-37 Due to the low severity of this h when it becomes available.	and DSA as a result of this d just feasible, because most o sources required for such an e DH1024 private key among AVX2 but not ADX extension 732 and CVE-2015-3193. Ope issue we are not issuing a ne	efect would be very difficult to f the work necessary to deduce attack would be significant. Hi i multiple clients, which is no least is like Intel Haswell (4th gene inSSL version 1.0.2-1.0.2m and w release of OpenSSL 1.1.0 at	o perform and are not ce information about a owever, for an attack on onger an option since CVE- ration). Note: The impact 1.1.0-1.1.0g are affected. this time. The fix will be		
CVE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	208.11.141.76	443	2019-01- 17T10:42:47.000Z	
handshake then OpenSSL as designed for the explicit work correctly if SSL_read	om version 1.0.2b) introduced a would move into the error sta it handshake functions (SSL_d I() or SSL_write() is called direc read()/SSL_write() is subseque	ate and would immediately fail lo_handshake(), SSL_accept() ctly. In that scenario, if the har	l if you attempted to continue and SSL_connect()), howeven dshake fails then a fatal error	the handshake. This works r due to a bug it does not will be returned in the		

initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would

have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2015-3185 208.11.141.76 https://nvd.nist.gov/vu 2015-07-20 443 2019-01-

In/detail/CVE-2015-

3185

17T10:42:47.000Z

Description:

The an_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

2017-11-02 208.11.141.76 CVF-2017-3736 https://nvd.nist.gov/vu 443 2019-01-

In/detail/CVE-2017-17T10:42:47.000Z

3736

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2017-3737 2017-12-07 208.11.141.167 443 2019-01https://nvd.nist.gov/vu

In/detail/CVE-2017-17T10:39:06.000Z

3737

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.167 443 2019-01-

In/detail/CVE-2016-

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.11.141.167 2019-01-443

In/detail/CVE-2015-

3183

17T10:39:06.000Z

17T10:39:06.000Z

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

https://nvd.nist.gov/vu CVE-2014-0226 2014-07-20 208.11.141.167 443 2019-01-

In/detail/CVE-2014-

0226

17T10:39:06.000Z

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3185 208.11.141.167 https://nvd.nist.gov/vu 2015-07-20 443 2019-01-In/detail/CVE-2015-

3185

17T10:39:06.000Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.1d does not consider that a Require	
directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass	
intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.	

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.11.141.167 443 2019-01-In/detail/CVE-2017-17T10:39:06.000Z 3736

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.11.141.167 443 2019-01-In/detail/CVE-2017-17T10:39:06.000Z

3738

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.75 443 2019-01-In/detail/CVE-2015-17T10:38:27.000Z

3185

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2016-0703 https://nvd.nist.gov/vu 2016-03-02 208.11.141.75 443 2019-01-In/detail/CVE-2016-17T10:38:27.000Z

0703

The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows manin-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

CVE-2015-3195 https://nvd.nist.gov/vu 2015-12-06 208 11 141 75 443 2019-01-

In/detail/CVE-2015-

3195

17T10:38:27.000Z

Description:

The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.75 443 2019-01-

In/detail/CVE-2016-

8743

17T10:38:27.000Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.75 443 2019-01-

> In/detail/CVE-2014-17T10:38:27.000Z

0226

_		
Desc		

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3183

https://nvd.nist.gov/vu ln/detail/CVE-2015-

3183

3197

3194

3185

2015-07-20

208.11.141.75

443

2019-01-17T10:38:27.000Z

Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2015-3197

https://nvd.nist.gov/vu In/detail/CVE-2015-

2016-02-14

208.11.141.75

443

2019-01-

17T10:38:27.000Z

Description:

ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.

CVE-2015-3194

Description:

https://nvd.nist.gov/vu ln/detail/CVE-20152015-12-06

208.11.141.75

443

2019-01-

17T10:38:27.000Z

crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.

CVE-2015-3185

https://nvd.nist.gov/vu ln/detail/CVE-20152015-07-20

199.47.156.89

443

2019-01-

17T10:34:10.000Z

_

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2015-3183

Description:

https://nvd.nist.gov/vu ln/detail/CVE-20152015-07-20

199.47.156.89

443

2019-01-

17T10:34:10.000Z

3183

invalid chunk-extension characters in modules/http/http_filters.c.

3736

3738

https://nvd.nist.gov/vu

In/detail/CVE-2017-

CVE-2017-3736

2017-11-02

199.47.156.89

443

2019-01-

17T10:34:10.000Z

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and

CVE-2017-3738

https://nvd.nist.gov/vu In/detail/CVE-20172017-12-07

199.47.156.89

443

2019-01-

17T10:34:10.000Z

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on

TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 199.47.156.89 443 2019-01-

In/detail/CVE-2017-17T10:34:10.000Z

3737

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 199.47.156.89 443 2019-01-In/detail/CVE-2014-17T10:34:10.000Z

0226

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 199 47 156 89 443 2019-01-

In/detail/CVE-2016-

8743

17T10:34:10.000Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2017-7529 https://nvd.nist.gov/vu 2017-07-13 66.193.233.167 443 2019-01-

In/detail/CVE-2017-

7529

17T06:34:42.000Z

Description:

Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.

CVE-2016-0703 https://nvd.nist.gov/vu 2016-03-02 63.240.88.6 2019-01-443

In/detail/CVE-2016-

0703

17T03:20:40.000Z

Description:

The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows manin-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 63.240.88.6 443 2019-01-

In/detail/CVE-2016-

8743

17T03:20:40.000Z

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

https://nvd.nist.gov/vu CVE-2016-8743 2017-07-27 64.128.99.203 443 2019-01-

In/detail/CVE-2016-

8743

17T02:49:38.000Z

D	
Descri	

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 64.128.99.203 443 2019-01-

> In/detail/CVE-2015-17T02:49:38.000Z

3185

Description:

The an_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2015-3195 https://nvd.nist.gov/vu 2015-12-06 64.128.99.203 443 2019-01-

> In/detail/CVE-2015-17T02:49:38.000Z

3195

Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.

CVE-2016-0703 https://nvd.nist.gov/vu 2016-03-02 64.128.99.203 443 2019-01-

In/detail/CVE-2016-17T02:49:38.000Z

0703

The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows manin-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

https://nvd.nist.gov/vu CVE-2015-3194 64.128.99.203 443 2019-01-2015-12-06

In/detail/CVE-2015-17T02:49:38.000Z

3194

Description:

cryptorsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 64.128.99.203 443 2019-01-

In/detail/CVE-2014-

0226

17T02:49:38.000Z

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3197 https://nvd.nist.gov/vu 2016-02-14 64.128.99.203 443 2019-01-

> In/detail/CVE-2015-17T02:49:38.000Z

3197

Description:

ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-inthe-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the

get_client_master_key and get_client_hello functions.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 64.128.99.203 443 2019-01-

In/detail/CVE-2015-

3183

17T02:49:38.000Z

Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and

invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2015-3185 2015-07-20 2019-01-64.128.99.92 443

https://nvd.nist.gov/vu In/detail/CVF-2015-17T02:38:34.000Z

	3185				
directive may be associate	red function in server/request, ed with an authorization settin ns in opportunistic circumstan	g rather than an authenticatio	n setting, which allows remot	e attackers to bypass	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	64.128.99.92	443	2019-01- 17T02:38:34.000Z
remote attackers to condu	ing implementation in the Apa ict HTTP request smuggling at naracters in modules/http/http.	ttacks via a crafted request, re			
CVE-2015-3197	https://nvd.nist.gov/vu In/detail/CVE-2015- 3197	2016-02-14	64.128.99.92	443	2019-01- 17T02:38:34.000Z
the-middle attackers to de	I.O.1 before 1.O.1r and 1.O.2 before tryptographic protection d get_client_hello functions.				
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	64.128.99.92	443	2019-01- 17T02:38:34.000Z
(heap-based buffer overflo	_status module in the Apache w), or possibly obtain sensitiv dling within the status_handler a_request.c.	e credential information or ex	recute arbitrary code, via a cra	afted request that triggers	
CVE-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	64.128.99.92	443	2019-01- 17T02:38:34.000Z
1.0.1m, and 1.0.2 before 1.0	ey function in s2_srvr.c in the S 0.2a accepts a nonzero CLIEN' determine the MASTER-KEY v CVE-2016-0800.	T-MASTER-KEY CLEAR-KEY-L	ENGTH value for an arbitrary	cipher, which allows man-	
CVE-2015-3195	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	64.128.99.92	443	2019-01- 17T02:38:34.000Z
1.0.2 before 1.0.2e mishan	IE implementation in crypto/as dles errors caused by malform memory by triggering a decod	ned X509_ATTRIBUTE data, v	which allows remote attackers		
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	64.128.99.92	443	2019-01- 17T02:38:34.000Z
lines and headers. Accept	Il releases prior to 2.2.32 and ing these different behaviors replication servers, either throughing and cache pollution.	represented a security conce	rn when httpd participates in	any chain of proxies or	
CVE-2015-3194	https://nvd.nist.gov/vu In/detail/CVE-2015- 3194	2015-12-06	64.128.99.92	443	2019-01- 17T02:38:34.000Z
	OpenSSL 1.0.1 before 1.0.1q ar application crash) via an RSA P				

CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	208.235.248.176	443	2019-01- 17T01:31:10.000Z
directive may be associate	red function in server/request. Ed with an authorization setting as in opportunistic circumstan	g rather than an authenticatio	n setting, which allows remote	e attackers to bypass	
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	208.235.248.176	443	2019-01- 17T01:31:10.000Z
(heap-based buffer overflo	_status module in the Apache ow), or possibly obtain sensitiv dling within the status_handler a_request.c.	e credential information or ex	ecute arbitrary code, via a cra	afted request that triggers	
CVE-2017-3736	https://nvd.nist.gov/vu In/detail/CVE-2017- 3736	2017-11-02	208.235.248.176	443	2019-01- 17T01:31:10.000Z
algorithms are affected. At are not believed likely. Att information about a private likely only accessible to a target private key in a scer	ng bug in the x86_64 Montgon nalysis suggests that attacks a acks against DH are consider e key may be performed offlin limited number of attackers. A nario with persistent DH parar e BMI1, BMI2 and ADX extens	gainst RSA and DSA as a resed just feasible (although venee. The amount of resources ratacker would additionally neters and a private key that	ult of this defect would be ver difficult) because most of the equired for such an attack wo need online access to an unp is shared between multiple cli	y difficult to perform and e work necessary to deduce uld be very significant and patched system using the ients. This only affects	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	208.235.248.176	443	2019-01- 17T01:31:10.000Z
lines and headers. Accept	I releases prior to 2.2.32 and ing these different behaviors replication servers, either through and cache pollution.	represented a security conce	rn when httpd participates in a	any chain of proxies or	
CVE-2017-3738	https://nvd.nist.gov/vu In/detail/CVE-2017- 3738	2017-12-07	208.235.248.176	443	2019-01- 17T01:31:10.000Z
are affected. Analysis suggested likely. Attacks ag private key may be perfort TLS to be meaningful, the 2016-0701. This only affect from this issue is similar to Fixed in OpenSSL 1.0.2n. I	n the AVX2 Montgomery mult gests that attacks against RSA ainst DH1024 are considered med offline. The amount of res server would have to share th ts processors that support the CVE-2017-3736, CVE-2017-37 Due to the low severity of this n when it becomes available.	and DSA as a result of this d just feasible, because most o sources required for such an a e DH1024 private key among AVX2 but not ADX extension 732 and CVE-2015-3193. Ope issue we are not issuing a ne	efect would be very difficult to f the work necessary to deduc attack would be significant. Hi i multiple clients, which is no least is like Intel Haswell (4th gene inSSL version 1.0.2-1.0.2m and w release of OpenSSL 1.1.0 at	o perform and are not ce information about a owever, for an attack on onger an option since CVE- ration). Note: The impact 1.1.0-1.1.0g are affected. this time. The fix will be	
CVE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	208.235.248.176	443	2019-01- 17T01:31:10.000Z
handshake then OpenSSL as designed for the explicit work correctly if SSL_read initial function call. If SSL_is passed without being dehave to be present that re-	om version 1.0.2b) introduced a would move into the error state thandshake functions (SSL_d) or SSL_write() is called directed()/SSL_write() is subsequencypted/encrypted directly frosulted in a call to SSL_read()/SFixed in OpenSSL 1.0.2n. OpenSSL 1.0.2n.	ate and would immediately faito_handshake(), SSL_accept(); ttly. In that scenario, if the har intly called by the application om the SSL/TLS record layer. SSL_write() being issued after	I if you attempted to continue and SSL_connect()), howeven dshake fails then a fatal error for the same SSL object then In order to exploit this issue a	the handshake. This works r due to a bug it does not will be returned in the it will succeed and the data n application bug would	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015-	2015-07-20	208.235.248.176	443	2019-01- 17T01:31:10.000Z

	3183					
remote attackers to cond	ding implementation in the Apa uct HTTP request smuggling at characters in modules/http/http_	tacks via a crafted request, re				
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	64.149.172.15	443	2019-01- 16T23:07:25.000Z	
directive may be associat	uired function in server/request. ted with an authorization setting ons in opportunistic circumstand	g rather than an authenticatio	n setting, which allows remot	e attackers to bypass		
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	64.149.172.15	443	2019-01- 16T23:07:25.000Z	
(heap-based buffer overfl	d_status module in the Apache ow), or possibly obtain sensitiv idling within the status_handler ia_request.c.	e credential information or ex	ecute arbitrary code, via a cr	afted request that triggers		
CVE-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	64.149.172.15	443	2019-01- 16T23:07:25.000Z	
1.0.1m, and 1.0.2 before 1.	ey function in s2_srvr.c in the S 0.2a accepts a nonzero CLIEN o determine the MASTER-KEY v CVE-2016-0800.	T-MASTÉR-KEY CLEAR-KEY-L	ENGTH value for an arbitrary	cipher, which allows man-		
CVE-2015-3197	https://nvd.nist.gov/vu In/detail/CVE-2015- 3197	2016-02-14	64.149.172.15	443	2019-01- 16T23:07:25.000Z	
the-middle attackers to d	1.0.1 before 1.0.1r and 1.0.2 before feat cryptographic protection and get_client_hello functions.					
CVE-2015-3195	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	64.149.172.15	443	2019-01- 16T23:07:25.000Z	
1.0.2 before 1.0.2e mishai	NE implementation in crypto/as ndles errors caused by malform memory by triggering a decod	ned X509_ATTRIBUTE data, v	which allows remote attackers			
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	64.149.172.15	443	2019-01- 16T23:07:25.000Z	
remote attackers to cond	ding implementation in the Apa uct HTTP request smuggling at characters in modules/http/http.	tacks via a crafted request, re				
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	64.149.172.15	443	2019-01- 16T23:07:25.000Z	
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.						

CVE-2015-3194	https://nvd.nist.gov/vu In/detail/CVE-2015- 3194	2015-12-06	64.149.172.15	443	2019-01- 16T23:07:25.000Z	
			emote attackers to cause a de a mask generation function p			
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	198.167.0.48	443	2019-01- 16T19:46:07.000Z	
lines and headers. Accepting	ng these different behaviors r blication servers, either throu	represented a security conce	espace accepted from reques in when httpd participates in a entional CGI mechanisms, and	any chain of proxies or		
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	192.131.76.25	443	2019-01- 16T19:33:07.000Z	
directive may be associated	d with an authorization setting	g rather than an authenticatio	2.4.x before 2.4.14 does not on setting, which allows remote of a module that relies on t	e attackers to bypass		
CVE-2017-3736	https://nvd.nist.gov/vu In/detail/CVE-2017- 3736	2017-11-02	192.131.76.25	443	2019-01- 16T19:33:07.000Z	
algorithms are affected. And are not believed likely. Atta information about a private likely only accessible to a lin target private key in a scen	alysis suggests that attacks a icks against DH are considera key may be performed offlin mited number of attackers. A ario with persistent DH parar	gainst RSA and DSA as a res ed just feasible (although very e. The amount of resources r in attacker would additionally neters and a private key that	OpenSSL before 1.0.2m and 1.1 ult of this defect would be ver a difficult) because most of the equired for such an attack wo need online access to an unpis shared between multiple cligeneration) and later or AMD	y difficult to perform and e work necessary to deduce uld be very significant and patched system using the ients. This only affects		
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	192.131.76.25	443	2019-01- 16T19:33:07.000Z	
lines and headers. Accepting	ng these different behaviors r blication servers, either throu	represented a security conce	espace accepted from reques n when httpd participates in a entional CGI mechanisms, and	any chain of proxies or		
CVE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	192.131.76.25	443	2019-01- 16T19:33:07.000Z	
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.						
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	192.131.76.25	443	2019-01- 16T19:33:07.000Z	
remote attackers to conduc		ttacks via a crafted request, re	4 does not properly parse ch elated to mishandling of large			

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 192.131.76.25 443 2019-01-In/detail/CVE-2017-16T19:33:07.000Z 3738 Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736. CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository. CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 192.131.76.25 443 2019-01-In/detail/CVE-2014-16T19:33:07.000Z 0226 Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers $improper\ scoreboard\ handling\ within\ the\ status_handler\ function\ in\ modules/generators/mod_status.c\ and\ the\ lua_ap_scoreboard_worker$ function in modules/lua/lua_request.c. CVE-2017-5647 https://nvd.nist.gov/vu 2017-04-17 192.131.72.236 443 2019-01-In/detail/CVE-2017-16T18:05:35.000Z 5647 Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C. CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 166.73.13.27 443 2019-01-In/detail/CVE-2016-16T17:39:27.000Z 8743 Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution. CVE-2017-3737 https://nvd.nist.gov/vu 2019-01-2017-12-07 166.73.13.27 443 In/detail/CVE-2017-16T17:39:27.000Z 3737 OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected. CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 2019-01-166.73.13.27 443 In/detail/CVE-2015-16T17:39:27.000Z 3183 Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c. CVE-2017-3738 2017-12-07 2019-01https://nvd.nist.gov/vu 166.73.13.27 443 In/detail/CVE-2017-16T17:39:27.000Z 3738

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0 when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 166.73.13.27 443 2019-01-

In/detail/CVE-2017- 16T17:39:27.000Z

3736

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 166.73.13.27 443 2019-01-

In/detail/CVE-2015- 16T17:39:27.000Z

3185

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 166.73.13.27 443 2019-01-

0226

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.235.248.131 443 2019-01-

In/detail/CVE-2015- 16T09:44:43.000Z

3185

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.235.248.131 443 2019-01-

In/detail/CVE-2014- 16T09:44:43.000Z

0226

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.235.248.131 443 2019-01-

In/detail/CVE-2017- 16T09:44:43.000Z

3738

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.10-11.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.10 at this time. The fix will be

included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.235.248.131 443

In/detail/CVE-2017-

In/detail/CVE-2017-

3736

2019-01-

16T09:44:43.000Z

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2017-3737 https://nvd.nist.gov/vu 3737

2017-12-07

208.235.248.131

443

2019-01-16T09:44:43.000Z

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.235.248.131 443 2019-01-

In/detail/CVE-2015-

3183

16T09:44:43.000Z

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2016-8743 2017-07-27 208.235.248.131 2019-01https://nvd.nist.gov/vu 443

In/detail/CVE-2016-

8743

16T09:44:43.000Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.235.248.157 443 2019-01-

In/detail/CVE-2017-

3736

16T09:42:14.000Z

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.235.248.157 443 2019-01-

In/detail/CVE-2014-

16T09:42:14.000Z

0226

Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.235.248.157 443 2019-01-

In/detail/CVE-2015-

16T09:42:14.000Z

3185 Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior. CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.235.248.157 443 2019-01-16T09:42:14.000Z In/detail/CVE-2017-3738 Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository. CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.235.248.157 443 2019-01-In/detail/CVE-2015-16T09:42:14.000Z 3183 Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c. CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 208.235.248.157 443 2019-01-In/detail/CVE-2017-16T09:42:14.000Z 3737 Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected. CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.235.248.157 443 2019-01-In/detail/CVE-2016-16T09:42:14.000Z 8743 Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution. CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.235.248.133 443 2019-01-In/detail/CVE-2017-16T09:32:11.000Z 3736 Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2017-3737	https://nvd.nist.gov/vu	2017-12-07	208.235.248.133	443	2019-01-
	In/detail/CVE-2017-				16T09:32:11.000Z
	2727				

3/

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.235.248.133 443 2019-01ln/detail/CVE-2016-8743 16T09:32:11.000Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.235.248.133 443 2019-01ln/detail/CVE-20140226 16T09:32:11.000Z

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.235.248.133 443 2019-01In/detail/CVE-2015- 16T09:32:11.000Z
3183

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.235.248.133 443 2019-01In/detail/CVE-2017- 16T09:32:11.000Z
3738

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.1.0 at the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0 when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.235.248.133 443 2019-01In/detail/CVE-2015- 16T09:32:11.000Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 166.73.92.88 443 2019-01In/detail/CVE-20153183 16708:24:14.000Z

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 166.73.92.88 443 2019-01-In/detail/CVE-2017- 16T08:24:14.000Z

3736

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2016-8743

https://nvd.nist.gov/vu ln/detail/CVE-20162017-07-27 166.73.92.88

443

2019-01-16T08:24:14.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

2017-12-07

CVE-2017-3737

https://nvd.nist.gov/vu

166.73.92.88

443

2019-01-16T08:24:14.000Z

In/detail/CVE-2017-

3737

3/3/

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2015-3185

https://nvd.nist.gov/vu ln/detail/CVE-20152015-07-20

166.73.92.88

443

2019-01-

16T08:24:14.000Z

3185

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2014-0226

https://nvd.nist.gov/vu In/detail/CVE-2014-

0226

3183

2014-07-20

166.73.92.88

443

2019-01-

16T08:24:14.000Z

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3738

https://nvd.nist.gov/vu 2017-12-07

In/detail/CVE-2017-

7 166.73.92.88

443

2019-01-

16T08:24:14.000Z

3738

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2015-3183

https://nvd.nist.gov/vu 2015-07-20 In/detail/CVE-2015208.11.141.192

443

2019-01-

16T07:13:12.000Z

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.11.141.192 443

In/detail/CVE-2017-

3736

2019-01-

16T07:13:12.000Z

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.192 443 2019-01-

In/detail/CVE-2015-

3185

16T07:13:12.000Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.11.141.192 443 2019-01-

In/detail/CVE-2017-

3738

16T07:13:12.000Z

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.192 2019-01-

In/detail/CVE-2014-

0226

443

16T07:13:12.000Z

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 208.11.141.192 443 2019-01-

In/detail/CVE-2017-

3737

16T07:13:12.000Z

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.192 443 2019-01-

In/detail/CVE-2016-

8743

16T07:13:12.000Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	208.11.141.196	443	2019-01- 16T07:05:38.000Z
lines and headers. Accep	all releases prior to 2.2.32 and iting these different behaviors replication servers, either throughting and cache pollution.	epresented a security conce	rn when httpd participates in	any chain of proxies or	
CVE-2017-3736	https://nvd.nist.gov/vu In/detail/CVE-2017- 3736	2017-11-02	208.11.141.196	443	2019-01- 16T07:05:38.000Z
algorithms are affected. A are not believed likely. At information about a privat likely only accessible to a target private key in a sce	ing bug in the x86_64 Montgoi nalysis suggests that attacks a tacks against DH are considera te key may be performed offlin- limited number of attackers. A enario with persistent DH paran ne BMI1, BMI2 and ADX extens	gainst RSA and DSA as a reset just feasible (although ver e. The amount of resources on n attacker would additionally neters and a private key that	sult of this defect would be ve y difficult) because most of the equired for such an attack wo need online access to an unj is shared between multiple cl	ry difficult to perform and e work necessary to deduce ould be very significant and patched system using the lients. This only affects	
CVE-2017-3738	https://nvd.nist.gov/vu In/detail/CVE-2017- 3738	2017-12-07	208.11.141.196	443	2019-01- 16T07:05:38.000Z
are affected. Analysis sug believed likely. Attacks as private key may be perfor TLS to be meaningful, the 2016-0701. This only affect from this issue is similar to Fixed in OpenSSL 1.0.2n.	in the AVX2 Montgomery multigests that attacks against RSA gainst DH1024 are considered growed offline. The amount of resessors what support the CVE-2017-3736, CVE-2017-37 Due to the low severity of this when it becomes available.	and DSA as a result of this clust feasible, because most coorces required for such an e DH1024 private key among AVX2 but not ADX extension 232 and CVE-2015-3193. Operissue we are not issuing a near the summer of	lefect would be very difficult to of the work necessary to dedu attack would be significant. H of multiple clients, which is no l ns like Intel Haswell (4th gene enSSL version 1.0.2-1.0.2m and tw release of OpenSSL 1.1.0 at	o perform and are not ce information about a owever, for an attack on longer an option since CVE- eration). Note: The impact d 1.1.0-1.1.0g are affected. t this time. The fix will be	
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	208.11.141.196	443	2019-01- 16T07:05:38.000Z
directive may be associat	ired function in server/request. ed with an authorization setting ins in opportunistic circumstand	g rather than an authenticatio	on setting, which allows remot	e attackers to bypass	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	208.11.141.196	443	2019-01- 16T07:05:38.000Z
remote attackers to cond	ling implementation in the Apa uct HTTP request smuggling at haracters in modules/http/http.	tacks via a crafted request, r			
CVE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	208.11.141.196	443	2019-01- 16T07:05:38.000Z
handshake then OpenSSI as designed for the explicit work correctly if SSL_rear initial function call. If SSL_is passed without being dhave to be present that re	om version 1.0.2b) introduced a L would move into the error sta- cit handshake functions (SSL_d d) or SSL_write() is called direc read()/SSL_write() is subseque lecrypted/encrypted directly from esulted in a call to SSL_read()/S I. Fixed in OpenSSL 1.0.2n. Open	te and would immediately fa o_handshake(), SSL_accept(ttly. In that scenario, if the ha ntly called by the application om the SSL/TLS record layer. SSL_write() being issued after	il if you attempted to continue) and SSL_connect()), howeve ndshake fails then a fatal erro I for the same SSL object then In order to exploit this issue a	e the handshake. This works or due to a bug it does not or will be returned in the or it will succeed and the data an application bug would	
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014-	2014-07-20	208.11.141.196	443	2019-01- 16T07:05:38.000Z

0226

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3736

https://nvd.nist.gov/vu In/detail/CVE-20172017-11-02 166.73.7.11

443

2019-01-16T07:00:56.000Z

3736

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2014-0226

https://nvd.nist.gov/vu In/detail/CVE-20142014-07-20

166.73.7.11

443

2019-01-

16T07:00:56.000Z

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2016-8743

https://nvd.nist.gov/vu 2017-07-27 In/detail/CVE-2016166.73.7.11

443

2019-01-

16T07:00:56.000Z

8743

0226

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2017-3737

https://nvd.nist.gov/vu ln/detail/CVE-20172017-12-07 166.73.7.11

443

2019-01-

16T07:00:56.000Z

3737

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2015-3183

https://nvd.nist.gov/vu In/detail/CVE-2015-

3183

3185

2015-07-20

166.73.7.11

443

2019-01-

16T07:00:56.000Z

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2015-3185

https://nvd.nist.gov/vu In/detail/CVE-20152015-07-20

166.73.7.11

443

2019-01-

16T07:00:56.000Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HADWARE OR DARDWARE OR HADWARE OR HA

16T05:41:31.000Z

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 2019-01-166.73.7.11 443 In/detail/CVE-2017-16T07:00:56.000Z Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository. CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 166.73.6.117 443 2019-01-In/detail/CVE-2017-16T05:41:31.000Z 3736 There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen. CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 166.73.6.117 443 2019-01-In/detail/CVE-2017-16T05:41:31.000Z 3737 Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected. CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 166.73.6.117 443 2019-01-In/detail/CVE-2016-16T05:41:31.000Z 8743 Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution. CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 166.73.6.117 443 2019-01-In/detail/CVE-2015-16T05:41:31.000Z 3183 Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c. CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 166.73.6.117 443 2019-01-In/detail/CVE-2014-16T05:41:31.000Z 0226 Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c. CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 166.73.6.117 443 2019-01-

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

In/detail/CVE-2015-

3185

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2017-3738

https://nvd.nist.gov/vu 2017-12-07

In/detail/CVE-2017-

166.73.6.117

443

2019-01-16T05:41:31.000Z

3738

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0 when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2016-8743

https://nvd.nist.gov/vu In/detail/CVE-20162017-07-27

166.73.6.118

443

2019-01-

16T05:40:54.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3183

https://nvd.nist.gov/vu In/detail/CVE-20152015-07-20

2015-07-20

166.73.6.118

443

2019-01-

16T05:40:54.000Z

3183

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2015-3185

https://nvd.nist.gov/vu In/detail/CVE-2015166.73.6.118

443

2019-01-

16T05:40:54.000Z

3185

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2017-3737

https://nvd.nist.gov/vu In/detail/CVE-2017-

2017-12-07

166.73.6.118

443

2019-01-

16T05:40:54.000Z

3737

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2014-0226

https://nvd.nist.gov/vu ln/detail/CVE-2014-

0226

2014-07-20

166.73.6.118

443

2019-01-

16T05:40:54.000Z

Description

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3736

https://nvd.nist.gov/vu

2017-11-02

166.73.6.118

443

2019-01-

In/detail/CVE-2017-16T05:40:54.000Z 3736 Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen. CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 166.73.6.118 443 2019-01-In/detail/CVE-2017-16T05:40:54.000Z 3738 Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository. CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.88 443 2019-01-In/detail/CVE-2014-16T00:59:46.000Z 0226 Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c. CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.11.141.88 443 2019-01-In/detail/CVE-2017-16T00:59:46.000Z 3736 Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen. CVE-2015-3183 2015-07-20 https://nvd.nist.gov/vu 208.11.141.88 443 2019-01-In/detail/CVE-2015-16T00:59:46.000Z 3183 The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c. CVE-2017-3738 208.11.141.88 443 2019-01-

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.11.141.88 443 2019-01In/detail/CVE-2017- 16T00:59:46.000Z
3738

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-11.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	208.11.141.88	443	2019-01- 16T00:59:46.000Z			
directive may be associate	d with an authorization setting	g rather than an authenticatio	2.4.x before 2.4.14 does not on setting, which allows remotice of a module that relies on t	e attackers to bypass				
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	208.11.141.88	443	2019-01- 16T00:59:46.000Z			
lines and headers. Accepting	ng these different behaviors r plication servers, either throu	represented a security conce	espace accepted from reques rn when httpd participates in a entional CGI mechanisms, and	any chain of proxies or				
CVE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	208.11.141.88	443	2019-01- 16T00:59:46.000Z			
handshake then OpenSSL as designed for the explicit work correctly if SSL_read(initial function call. If SSL_ri is passed without being de have to be present that res	would move into the error sta t handshake functions (SSL_d) or SSL_write() is called directed ead()/SSL_write() is subseque crypted/encrypted directly fro	ate and would immediately fai to_handshake(), SSL_accept() sttly. In that scenario, if the har whitly called by the application om the SSL/TLS record layer. SSL_write() being issued after	he intent was that if a fatal err I if you attempted to continue and SSL_connect()), howeven dshake fails then a fatal error for the same SSL object then In order to exploit this issue a having already received a fat	the handshake. This works r due to a bug it does not will be returned in the it will succeed and the data n application bug would				
CVE-2017-3736	https://nvd.nist.gov/vu In/detail/CVE-2017- 3736	2017-11-02	66.193.233.175	80	2019-01- 12T21:58:58.000Z			
algorithms are affected. An are not believed likely. Atta information about a private likely only accessible to a li target private key in a scen	allysis suggests that attacks a acks against DH are considers key may be performed offlin imited number of attackers. A nario with persistent DH parar	gainst RSA and DSA as a resed just feasible (although vene. The amount of resources rattacker would additionally neters and a private key that	OpenSSL before 1.0.2m and 1.1 ult of this defect would be ver y difficult) because most of the equired for such an attack wo need online access to an unp is shared between multiple cli generation) and later or AMD	y difficult to perform and e work necessary to deduce uld be very significant and patched system using the ients. This only affects				
CVE-2017-3738	https://nvd.nist.gov/vu In/detail/CVE-2017- 3738	2017-12-07	66.193.233.175	80	2019-01- 12T21:58:58.000Z			
are affected. Analysis sugg believed likely. Attacks aga private key may be perforn TLS to be meaningful, the s 2016-0701. This only affect from this issue is similar to Fixed in OpenSSL 1.0.2n. D	Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on ILS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be nocluded in OpenSSL 1.1.0 when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.							
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	66.193.233.175	80	2019-01- 12T21:58:58.000Z			
(heap-based buffer overflo	w), or possibly obtain sensitiv ling within the status_handle	e credential information or ex	llows remote attackers to cau secute arbitrary code, via a cra ors/mod_status.c and the lua	afted request that triggers				
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015-	2015-07-20	66.193.233.175	80	2019-01- 12T21:58:58.000Z			

	3185				
	3103				
directive may be associate	ed function in server/request d with an authorization setting is in opportunistic circumstan	g rather than an authenticatio	n setting, which allows remot	e attackers to bypass	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	66.193.233.175	80	2019-01- 12T21:58:58.000Z
remote attackers to condu-	ng implementation in the Apa ct HTTP request smuggling at aracters in modules/http/http.	ttacks via a crafted request, r			
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	66.193.233.175	80	2019-01- 12T21:58:58.000Z
lines and headers. Accepti	I releases prior to 2.2.32 and ng these different behaviors replication servers, either througing and cache pollution.	represented a security conce	rn when httpd participates in	any chain of proxies or	
CVE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	66.193.233.175	80	2019-01- 12T21:58:58.000Z
handshake then OpenSSL as designed for the explicit work correctly if SSL_read initial function call. If SSL_r is passed without being de have to be present that res	m version 1.0.2b) introduced a would move into the error state thandshake functions (SSL_d) or SSL_write() is called directed()/SSL_write() is subsequencypted/encrypted directly froulted in a call to SSL_read()/SFixed in OpenSSL 1.0.2n. Open	ate and would immediately fa lo_handshake(), SSL_accept(ctly. In that scenario, if the har rintly called by the application om the SSL/TLS record layer. SSL_write() being issued after	il if you attempted to continue and SSL_connect()), howevendshake fails then a fatal erro for the same SSL object ther In order to exploit this issue a	the handshake. This works r due to a bug it does not r will be returned in the it will succeed and the data an application bug would	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	63.128.95.117	443	2019-01- 12T05:29:55.914Z
	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via			which makes it easier for	
CVE-2016-0800	https://nvd.nist.gov/vu In/detail/CVE-2016- 0800	2016-03-01	205.219.236.229	443	2019-01- 12T04:56:14.036Z
message before establishing	ed in OpenSSL before 1.0.1s a ng that a client possesses cer ng a Bleichenbacher RSA pao	tain plaintext RSA data, which	h makes it easier for remote a		
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	205.219.236.229	443	2019-01- 12T04:56:14.036Z
	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	198.246.154.136	443	2019-01- 12T02:17:11.556Z
	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via			which makes it easier for	

CVE_2014_3566 Parce Parc								
The SSI, protocol 30, as used in OpenSSI, through 10.1 and other products, uses more determinate. CBC pedding, which makes it easier for main-in-the-middle activate to a bits an electric data via a pedding-graded activate, as an in-more products, uses more determinate. CBC pedding, which makes it easier for main-in-the-middle activates to obtain clicaritat data via a pedding and either products, uses more determinate. CBC pedding, which makes it easier for main-in-the-middle activates to obtain clicaritat data via a pedding and either products, uses more determinate. CBC pedding, which makes it easier for main-in-the-middle activates to obtain clicaritat data via a pedding and either products, uses more determinate. CBC pedding, which makes it easier for main-in-the-middle activates to obtain clicaritat data via a pedding-oracle attack, as the "POODLE" issue. CVE-2014-3566	CVE-2014-3566	In/detail/CVE-2014-	2014-10-14	12.16.165.127	443			
Description: The SSL protocol 30, as used in OpenSSL through 10.11 and other products, uses nondeterministic CBC padding, which makes it easier for marker-the-middle attractives to obtaind clearance data with a padding-oracle attrack, also the "POODLE" issue. CVE 2014-3566 https://much nist gov/vu	The SSL protocol 3.0, as u				which makes it easier for			
The SSI, protocol 3.0, as used in OpenSSL through 1.0.1 and other products, uses nondeterministic CBC padding, which makes it easier for main-info-minidal actives to obtain clearted data via a padding-norcial attack, also the ProDUCE* issue. CVE-2014-3566	CVE-2014-3566	In/detail/CVE-2014-	2014-10-14	12.16.164.14	443			
In/detail/CVE-2014- 3566 Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1 and other products, uses nondeterministic CBC padding, which makes it easier for manier-in-the-middle attackers to obtain clearext data via a padding-oracle attack, as the "POODLE" issue. CVE-2015-3183 Intips://mvd.nist.gov/vu	The SSL protocol 3.0, as u				which makes it easier for			
The SSL protocol 3.0, as used in OpenSSL through 1.0.1 and other products, uses nondesterministic CBC padding, which makes it easier for man in-the middle datackers to obtain clearbox data via a padding-oracle attack, ake the "POODLE" issue. CVE-2015-3183	CVE-2014-3566	In/detail/CVE-2014-	2014-10-14	50.58.10.133	443			
In/detail/CVE-2015-3183 Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mischandling of large chunk-size values and invalid chunk-excension characters in moduleshynthrib_Effers. CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 208.11.141.76 80 2019-01-11722-50-41.0002 Description: OpenSSL 1.0.2 (starting from version 10.2.b) introduced an "error state" mechanism. The Intent was that if a fatal error occurred during a handshake from OpenSSL version of the explicit handshake from the OpenSSL code and would immediately fall if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_Inandshake(), SSL_accept) and SSL_consec(1)), however due to a bug it does not work correctly if SSL_preadily OSSL_write() is called directly. In that scenario, if the handshake falls then a fatal error will returned in the initial function call. If SSL_readily SSL_write() is called directly. In that scenario, if the handshake falls then a fatal error will will succeed and the data is passed without being decrypted-incrypted directly trom the SSL/TIS record layer. In order to exploit this issue in application bug would have to be present that resulted in a call to SSL_readily SSL_write() being issued after having already received a fatal error. OpenSSL version 10.20-10.20 are affected. Fixed in OpenSSL 10.20, OpenSSL 11.01 is not affected. CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.11.141.76 80 2019-01-11722-50-41.0002 Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against RSA and DSA as a result of this defect would be	The SSL protocol 3.0, as u				which makes it easier for			
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c. CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 208.11.141.76 80 2019-01-11722:50.41.000Z 3737 Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake the OpenSSL would move into the error state and would immediately fall if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_acceptl) and SSL_connect(t), however due to a bug it does not work correctly if SSL_read()/SSL_write() is called directly. In that scenario, if the handshake falls handshake than a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted encrypted directly from the SSLT.Ts record legyloid this issue an affected. See the properties of the propert	CVE-2015-3183	In/detail/CVE-2015-	2015-07-20	208.11.141.76	80			
In/detail/CVE-2017- 3737 Description: OpenSSL 1.0.2 (starting from version 10.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fall if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_0.5 handshaked), SSL_accept) and SSL_connect()), however due to a bug it does not work correctly if SSL_readily SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issucceed and play would have to be present that resulted in a call to SSL_readilySSL_write() being issued after having already received a fatal error. OpenSSL version 1.02-b1.02 m are affected. Fixed in OpenSSL 10.2n. OpenSSL 1.10 is not affected. CVE-2017-3738 https://rwd.nist.gov/vu 2017-12-07 208.11.141.76 80 2019-01-11722:50.41.000Z 3738 Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intell Haswall (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 10.2-10.2m and 11.0-11.0g are affected. Fixed in OpenSSL 1.10h wh	The chunked transfer codi remote attackers to condu	ct HTTP request smuggling at	ttacks via a crafted request, re					
OpenSSL 1.0.2 (starting from version 10.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fall if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake), SSL_accept() and SSL_connect(), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake falls then a fatal error will be returned in the initial function call. If SSL_read() SSL_write() is called directly. In that scenario, if the handshake falls then a fatal error will be returned in the initial function call. If SSL_read() SSL_write() being long the handshake falls then a fatal error will be returned in the initial function call. If SSL_read() SSL_write() being listed a fatal error. OpenSSL to exist the initial spassed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected. CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.11.141.76 80 2019-01-1172:50-41.0002 1172:50-41.0	CVE-2017-3737	In/detail/CVE-2017-	2017-12-07	208.11.141.76	80			
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-11.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository. CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.76 80 2019-01- 11722:50:41.000Z Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker	OpenSSL 1.0.2 (starting from handshake then OpenSSL as designed for the explicit work correctly if SSL_read initial function call. If SSL_is passed without being dehave to be present that research.	would move into the error state thandshake functions (SSL_d () or SSL_write() is called direct read()/SSL_write() is subseque scrypted/encrypted directly from a call to SSL_read()/Sulted in a call to SSL_read()	ate and would immediately failo_handshake(), SSL_accept()ctly. In that scenario, if the hareintly called by the application om the SSL/TLS record layer. SSL_write() being issued after	il if you attempted to continue and SSL_connect()), howevendshake fails then a fatal error for the same SSL object then In order to exploit this issue a	the handshake. This works r due to a bug it does not r will be returned in the it will succeed and the data an application bug would			
There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository. CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.76 80 2019-01-11722:50:41.000Z Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker	CVE-2017-3738	In/detail/CVE-2017-	2017-12-07	208.11.141.76	80			
In/detail/CVE-2014- 0226 Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker	There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be							
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker	CVE-2014-0226	In/detail/CVE-2014-	2014-07-20	208.11.141.76	80			
	Race condition in the mod (heap-based buffer overflo improper scoreboard hand	ow), or possibly obtain sensitiv dling within the status_handle	e credential information or ex	cecute arbitrary code, via a cra	afted request that triggers			

CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	208.11.141.76	80	2019-01- 11T22:50:41.000Z		
directive may be associate	red function in server/request ed with an authorization settin ns in opportunistic circumstan	g rather than an authenticatio	n setting, which allows remot	e attackers to bypass			
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	208.11.141.76	80	2019-01- 11T22:50:41.000Z		
lines and headers. Accept	Il releases prior to 2.2.32 and ing these different behaviors opplication servers, either throuting and cache pollution.	represented a security conce	rn when httpd participates in	any chain of proxies or			
CVE-2017-3736	https://nvd.nist.gov/vu In/detail/CVE-2017- 3736	2017-11-02	208.11.141.76	80	2019-01- 11T22:50:41.000Z		
algorithms are affected. At are not believed likely. Att information about a private likely only accessible to a target private key in a sce	ng bug in the x86_64 Montgo nalysis suggests that attacks a acks against DH are consider e key may be performed offlin limited number of attackers. A nario with persistent DH parar le BMI1, BMI2 and ADX extens	gainst RSA and DSA as a resed just feasible (although vene. The amount of resources ranattacker would additionally neters and a private key that	ult of this defect would be ver difficult) because most of the equired for such an attack wo need online access to an un- is shared between multiple cl	ry difficult to perform and e work necessary to deduce uld be very significant and patched system using the ients. This only affects			
CVE-2017-7529	https://nvd.nist.gov/vu In/detail/CVE-2017- 7529	2017-07-13	66.193.233.167	80	2019-01- 11T18:21:17.000Z		
	oup to and including 1.13.2 are e information triggered by spe		w vulnerability in nginx range	filter module resulting into			
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	192.131.76.202	443	2019-01- 11T12:45:22.138Z		
	ised in OpenSSL through 1.0.1 irs to obtain cleartext data via		, 5.	which makes it easier for			
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	192.131.76.78	443	2019-01- 11T12:34:21.489Z		
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.							
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	192.131.76.203	443	2019-01- 11T12:20:21.534Z		
	ised in OpenSSL through 1.0.1 irs to obtain cleartext data via			which makes it easier for			
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	50.58.10.161	443	2019-01- 10T22:34:40.871Z		
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for			
		-					

CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	50.58.10.165	443	2019-01- 10T22:17:34.853Z
		and other products, uses nor a padding-oracle attack, aka t	ndeterministic CBC padding, v he "POODLE" issue.	which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	12.168.132.240	443	2019-01- 10T21:56:48.732Z
		and other products, uses nor a padding-oracle attack, aka t	ndeterministic CBC padding, v he "POODLE" issue.	which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	208.11.141.9	443	2019-01- 10T20:16:20.205Z
		and other products, uses nor a padding-oracle attack, aka t	ndeterministic CBC padding, v he "POODLE" issue.	which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	208.11.141.38	443	2019-01- 10T20:13:49.019Z
		and other products, uses nor a padding-oracle attack, aka t	ndeterministic CBC padding, v he "POODLE" issue.	which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	192.131.73.13	443	2019-01- 10T17:25:25.893Z
		and other products, uses nor a padding-oracle attack, aka t	ndeterministic CBC padding, v he "POODLE" issue.	which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	192.131.72.240	443	2019-01- 10T17:12:32.162Z
		and other products, uses nor a padding-oracle attack, aka t	ndeterministic CBC padding, v he "POODLE" issue.	which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	64.128.99.240	443	2019-01- 10T16:05:43.264Z
		and other products, uses nor a padding-oracle attack, aka t	ndeterministic CBC padding, v he "POODLE" issue.	vhich makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	208.235.248.43	443	2019-01- 10T13:48:42.367Z
		and other products, uses nor a padding-oracle attack, aka t	ndeterministic CBC padding, v he "POODLE" issue.	vhich makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	12.16.164.65	443	2019-01- 10T13:02:05.566Z
Description: The SSL protocol 3.0, as use	ed in OpenSSL through 1.0.1i	and other products, uses nor	ndeterministic CBC padding, v	which makes it easier for	

man in the middle etter-	ore to obtain cloartout data : :-	a nadding oraclo attack site	the "POOD! E" issue		
тпан-ш-ше-тпіаате аттаск	ers to obtain cleartext data via	a pauding-oracie attack, aka	me POODLE ISSUE.		
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	184.170.226.96	443	2019-01- 10T10:17:20.571Z
	used in OpenSSL through 1.0.1i ers to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	64.128.99.48	443	2019-01- 10T07:02:03.521Z
	used in OpenSSL through 1.0.1i ers to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	12.44.79.219	443	2019-01- 10T04:37:51.960Z
	used in OpenSSL through 1.0.1i ers to obtain cleartext data via			which makes it easier for	
CVE-2016-0800	https://nvd.nist.gov/vu In/detail/CVE-2016- 0800	2016-03-01	204.95.150.234	443	2019-01- 10T04:23:05.368Z
message before establish	ised in OpenSSL before 1.0.1s a hing that a client possesses cer ging a Bleichenbacher RSA pac	tain plaintext RSA data, whic	h makes it easier for remote a		
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	204.95.150.234	443	2019-01- 10T04:23:05.368Z
	used in OpenSSL through 1.0.1i ers to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	204.95.150.215	443	2019-01- 10T03:58:54.250Z
	used in OpenSSL through 1.0.1i ers to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	198.246.154.221	443	2019-01- 10T00:59:08.126Z
	used in OpenSSL through 1.0.1i ers to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	12.168.132.183	443	2019-01- 09T20:49:00.865Z
	used in OpenSSL through 1.0.1i ers to obtain cleartext data via			which makes it easier for	
CVE-2016-0777	https://nvd.nist.gov/vu In/detail/CVE-2016- 0777	2016-04-01	65.206.30.70	22	2019-01- 09T18:52:22.131Z

ensitive information fro	m process memory by requestir			remote servers to ob- reading a private key.	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	204.95.150.252	443	2019-01- 09T16:47:04.649Z
	used in OpenSSL through 1.0.1i kers to obtain cleartext data via			ng, which makes it eas	sier for
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	12.168.133.81	443	2019-01- 09T16:33:20.094Z
	used in OpenSSL through 1.0.1i kers to obtain cleartext data via			ng, which makes it eas	sier for
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	192.131.72.207	443	2019-01- 09T16:10:06.771Z
	used in OpenSSL through 1.0.1i kers to obtain cleartext data via			ng, which makes it eas	sier for
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	192.131.72.172	443	2019-01- 09T16:03:18.186Z
Description: The SSL protocol 3.0, as	used in OpenSSL through 1.0.1i	and other products, use	as nondatarministic CRC naddi	ng, which makes it eas	sier for
nan-in-the-middle attack	kers to obtain cleartext data via			3.	
nan-in-the-middle attack				443	2019-01- 09T15:56:46.378Z
CVE-2014-3566 Description: The SSL protocol 3.0, as	https://nvd.nist.gov/vu In/detail/CVE-2014-	a padding-oracle attack, 2014-10-14 and other products, use	, aka the "POODLE" issue. 12.168.133.229 es nondeterministic CBC paddi	443	2019-01- 09T15:56:46.378Z
CVE-2014-3566 Description: The SSL protocol 3.0, as	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	a padding-oracle attack, 2014-10-14 and other products, use	, aka the "POODLE" issue. 12.168.133.229 es nondeterministic CBC paddi	443	2019-01- 09T15:56:46.378Z
excription: he SSL protocol 3.0, as nan-in-the-middle attack	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566 s used in OpenSSL through 1.0.1ixers to obtain cleartext data via https://nvd.nist.gov/vu In/detail/CVE-2014-	a padding-oracle attack, 2014-10-14 and other products, use a padding-oracle attack, 2014-10-14 and other products, use	aka the "POODLE" issue. 12.168.133.229 es nondeterministic CBC paddir, aka the "POODLE" issue. 166.73.13.54	443 ng, which makes it eas 443	2019-01- 09T15:56:46.378Z sier for 2019-01- 09T15:27:05.701Z
excription: he SSL protocol 3.0, as nan-in-the-middle attack	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566 sused in OpenSSL through 1.0.1i kers to obtain cleartext data via https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	a padding-oracle attack, 2014-10-14 and other products, use a padding-oracle attack, 2014-10-14 and other products, use	aka the "POODLE" issue. 12.168.133.229 es nondeterministic CBC paddir, aka the "POODLE" issue. 166.73.13.54	443 ng, which makes it eas 443	2019-01- 09T15:56:46.378Z sier for 2019-01- 09T15:27:05.701Z
Description: The SSL protocol 3.0, as nan-in-the-middle attack	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566 sused in OpenSSL through 1.0.1i kers to obtain cleartext data via https://nvd.nist.gov/vu In/detail/CVE-2014- 3566 sused in OpenSSL through 1.0.1i kers to obtain cleartext data via https://nvd.nist.gov/vu In/detail/CVE-2014-	a padding-oracle attack, 2014-10-14 and other products, use a padding-oracle attack, 2014-10-14 and other products, use a padding-oracle attack, 2014-10-14 and other products, use a padding-oracle attack, 2014-10-14	aka the "POODLE" issue. 12.168.133.229 es nondeterministic CBC paddir, aka the "POODLE" issue. 166.73.13.54 es nondeterministic CBC paddir, aka the "POODLE" issue. 170.90.16.206	443 ng, which makes it eas 443 ng, which makes it eas 443	2019-01- 09T15:56:46.378Z Sier for 2019-01- 09T15:27:05.701Z
Description: The SSL protocol 3.0, as nan-in-the-middle attack	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566 sused in OpenSSL through 1.0.1i kers to obtain cleartext data via https://nvd.nist.gov/vu In/detail/CVE-2014- 3566 sused in OpenSSL through 1.0.1i kers to obtain cleartext data via https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	a padding-oracle attack, 2014-10-14 and other products, use a padding-oracle attack, 2014-10-14 and other products, use a padding-oracle attack, 2014-10-14 and other products, use a padding-oracle attack, 2014-10-14	aka the "POODLE" issue. 12.168.133.229 es nondeterministic CBC paddir, aka the "POODLE" issue. 166.73.13.54 es nondeterministic CBC paddir, aka the "POODLE" issue. 170.90.16.206	443 ng, which makes it eas 443 ng, which makes it eas 443	2019-01- 09T15:56:46.378Z Sier for 2019-01- 09T15:27:05.701Z
Description: The SSL protocol 3.0, as nan-in-the-middle attack Description:	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566 sused in OpenSSL through 1.0.1i kers to obtain cleartext data via https://nvd.nist.gov/vu In/detail/CVE-2014- 3566 sused in OpenSSL through 1.0.1i kers to obtain cleartext data via https://nvd.nist.gov/vu In/detail/CVE-2014- 3566 sused in OpenSSL through 1.0.1i kers to obtain cleartext data via https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	a padding-oracle attack, 2014-10-14 and other products, use a padding-oracle attack, 2014-10-14 and other products, use a padding-oracle attack, 2014-10-14 and other products, use a padding-oracle attack, 2014-10-14	aka the "POODLE" issue. 12.168.133.229 es nondeterministic CBC paddir, aka the "POODLE" issue. 166.73.13.54 es nondeterministic CBC paddir, aka the "POODLE" issue. 170.90.16.206 es nondeterministic CBC paddir, aka the "POODLE" issue. 50.58.9.169	443 ng, which makes it eas 443 ng, which makes it eas 443 ng, which makes it eas 443	2019-01- 09T15:56:46.378Z sier for 2019-01- 09T15:27:05.701Z sier for 2019-01- 09T10:29:37.193Z sier for 2019-01- 09T09:51:01.944Z

	3566							
	used in OpenSSL through 1.0.1i ers to obtain cleartext data via			which makes it easier for				
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	204.95.150.218	443	2019-01- 09T02:59:41.140Z			
	used in OpenSSL through 1.0.1i ers to obtain cleartext data via			which makes it easier for				
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	208.235.248.86	443	2019-01- 09T00:59:37.385Z			
	used in OpenSSL through 1.0.1i ers to obtain cleartext data via			which makes it easier for				
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	208.235.248.122	443	2019-01- 09T00:44:36.592Z			
	used in OpenSSL through 1.0.1i ers to obtain cleartext data via			which makes it easier for				
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	209.211.226.237	443	2019-01- 08T18:21:09.838Z			
	used in OpenSSL through 1.0.1i ers to obtain cleartext data via			which makes it easier for				
CVE-2015-0204	https://nvd.nist.gov/vu In/detail/CVE-2015- 0204	2015-01-08	209.211.226.236	443	2019-01- 08T18:20:59.506Z			
The SSL protocol 3.0, as	Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.							
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	209.211.226.236	443	2019-01- 08T18:20:59.506Z			
Description: The SSL protocol 3.0, as	In/detail/CVE-2014-	and other products, uses no	ndeterministic CBC padding, v					
Description: The SSL protocol 3.0, as	In/detail/CVE-2014- 3566 used in OpenSSL through 1.0.1i	and other products, uses no	ndeterministic CBC padding, v					
Description: The SSL protocol 3.0, as man-in-the-middle attacked CVE-2014-3566 Description: The SSL protocol 3.0, as	In/detail/CVE-2014- 3566 used in OpenSSL through 1.0.1i ers to obtain cleartext data via https://nvd.nist.gov/vu In/detail/CVE-2014-	i and other products, uses not a padding-oracle attack, aka t 2014-10-14	ndeterministic CBC padding, v the "POODLE" issue. 166.73.6.60 ndeterministic CBC padding, v	which makes it easier for 443	08T18:20:59.506Z			
Description: The SSL protocol 3.0, as in an in-the-middle attacked CVE-2014-3566 Description: The SSL protocol 3.0, as in a second control of the solution in	In/detail/CVE-2014- 3566 used in OpenSSL through 1.0.1i ers to obtain cleartext data via https://nvd.nist.gov/vu In/detail/CVE-2014- 3566 used in OpenSSL through 1.0.1i	i and other products, uses not a padding-oracle attack, aka t 2014-10-14	ndeterministic CBC padding, v the "POODLE" issue. 166.73.6.60 ndeterministic CBC padding, v	which makes it easier for 443	08T18:20:59.506Z			

CVE-2015-0204	https://nvd.nist.gov/vu In/detail/CVE-2015- 0204	2015-01-08	204.95.150.47	443	2019-01- 08T17:18:18.765Z
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	192.131.76.40	443	2019-01- 08T16:03:15.734Z
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	204.95.150.253	443	2019-01- 08T15:46:27.220Z
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	50.58.10.164	443	2019-01- 08T14:46:14.351Z
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	50.58.10.162	443	2019-01- 08T14:35:35.293Z
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for	
CVE-2016-0800	https://nvd.nist.gov/vu In/detail/CVE-2016- 0800	2016-03-01	209.163.213.137	443	2019-01- 08T10:38:00.297Z
message before establish	sed in OpenSSL before 1.0.1s a ing that a client possesses cer jing a Bleichenbacher RSA pao	tain plaintext RSA data, which	h makes it easier for remote a		
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	209.163.213.137	443	2019-01- 08T10:38:00.297Z
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	209.163.213.104	443	2019-01- 08T10:34:00.415Z
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	209.163.213.138	443	2019-01- 08T10:22:18.470Z

Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue. CVE-2015-0204	:44:28.564Z 1- :25:08.223Z
In/detail/CVE-2014-3566 Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue. CVE-2015-0204 https://nvd.nist.gov/vu 2015-01-08 12.16.165.87 443 2019-0 1n/detail/CVE-2015-0204 Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue. CVE-2015-4000 https://nvd.nist.gov/vu 2015-05-20 12.16.165.87 443 2019-0 1n/detail/CVE-2015-4000 Description: The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue. CVE-2014-3566 https://nvd.nist.gov/vu 2014-10-14 12.16.165.87 443 2019-0	1- :25:08.223Z
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue. CVE-2015-0204	:25:08.223Z 1-
In/detail/CVE-2015- 0204 Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for nan-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue. CVE-2015-4000 https://nvd.nist.gov/vu 2015-05-20 12.16.165.87 443 2019-0: https://nvd.nist.gov/vu 2015-05-20 12.16.165.87 443 2019-0: OBST04: Description: The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue. CVE-2014-3566 https://nvd.nist.gov/vu 2014-10-14 12.16.165.87 443 2019-0:	:25:08.223Z 1-
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue. CVE-2015-4000 https://nvd.nist.gov/vu 2015-05-20 12.16.165.87 443 2019-0: ln/detail/CVE-2015-4000 Description: The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue. CVE-2014-3566 https://nvd.nist.gov/vu 2014-10-14 12.16.165.87 443 2019-0:	
In/detail/CVE-2015- 4000 Description: The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE eplaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue. CVE-2014-3566 https://nvd.nist.gov/vu 2014-10-14 12.16.165.87 443 2019-0	
The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE eplaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue. CVE-2014-3566 https://nvd.nist.gov/vu 2014-10-14 12.16.165.87 443 2019-0	
· · · · · · · · · · · · · · · · · · ·	
3566	1- :25:08.223Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.	
CVE-2014-3566 https://nvd.nist.gov/vu 2014-10-14 12.16.165.142 443 2019-0 In/detail/CVE-2014- 3566 08T04:	1- :20:58.102Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.	
CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.73 80 2019-0 In/detail/CVE-2014- 0226 07T01:3	1- 37:50.238Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers mproper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.	
CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.73 80 2019-0 In/detail/CVE-2016- 8743	1- 37:50.238Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response ines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.	
CVE-2015-3194 https://nvd.nist.gov/vu 2015-12-06 208.11.141.73 80 2019-0 In/detail/CVE-2015- 3194	1- 37:50.238Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL	

pointer dereference and ap	oplication crash) via an RSA P	SS ASN.1 signature that lacks	a mask generation function p	parameter.		
CVE-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	208.11.141.73	80	2019-01- 07T01:37:50.238Z	
1.0.1m, and 1.0.2 before 1.0.2	2a accepts a nonzero CLIENT letermine the MASTER-KEY v	-MASTER-KEY CLEAR-KEY-L	nSSL before 0.9.8zf, 1.0.0 bef ENGTH value for an arbitrary ext data by leveraging a Bleic	cipher, which allows man-		
CVE-2015-3195	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	208.11.141.73	80	2019-01- 07T01:37:50.238Z	
1.0.2 before 1.0.2e mishand		ed X509_ATTRIBUTE data, v	efore 0.9.8zh, 1.0.0 before 1.0. which allows remote attackers IS application.			
CVE-2015-3197	https://nvd.nist.gov/vu In/detail/CVE-2015- 3197	2016-02-14	208.11.141.73	80	2019-01- 07T01:37:50.238Z	
the-middle attackers to defe			e of disabled ciphers, which romputations on SSLv2 traffic,			
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	208.11.141.73	80	2019-01- 07T01:37:50.238Z	
remote attackers to conduc		tacks via a crafted request, re	4 does not properly parse ch elated to mishandling of large			
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	208.11.141.73	80	2019-01- 07T01:37:50.238Z	
directive may be associated	d with an authorization setting	rather than an authenticatio	2.4.x before 2.4.14 does not on setting, which allows remote of a module that relies on t	e attackers to bypass		
CVE-2017-3738	https://nvd.nist.gov/vu In/detail/CVE-2017- 3738	2017-12-07	208.11.141.88	80	2019-01- 06T12:13:29.238Z	
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 11.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0 when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.						
CVE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	208.11.141.88	80	2019-01- 06T12:13:29.238Z	
handshake then OpenSSL vas designed for the explicit	would move into the error sta handshake functions (SSL_d	te and would immediately fai o_handshake(), SSL_accept()	he intent was that if a fatal err I if you attempted to continue and SSL_connect()), however idshake fails then a fatal error	the handshake. This works r due to a bug it does not		

		enSSL 1.1.0 is not affec		a fatal error. OpenSSL ve	
VE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	208.11.141.88	80	2019-01- 06T12:13:29.238Z
rective may be associ	quired function in server/request. ated with an authorization setting tions in opportunistic circumstand	g rather than an authe	ntication setting, which allows re	emote attackers to bypass	5
VE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	208.11.141.88	80	2019-01- 06T12:13:29.238Z
eap-based buffer ove	od_status module in the Apache rflow), or possibly obtain sensitiv andling within the status_handler /lua_request.c.	e credential informatio	on or execute arbitrary code, via	a crafted request that trig	ggers
VE-2017-3736	https://nvd.nist.gov/vu In/detail/CVE-2017- 3736	2017-11-02	208.11.141.88	80	2019-01- 06T12:13:29.238Z
gorithms are affected, re not believed likely, formation about a prival kely only accessible to irget private key in a s	ating bug in the x86_64 Montgor Analysis suggests that attacks a Attacks against DH are considered ate key may be performed offling a limited number of attackers. A cenario with persistent DH parant the BMI1, BMI2 and ADX extens	gainst RSA and DSA a ed just feasible (althou e. The amount of reso n attacker would addit neters and a private ke	is a result of this defect would b gh very difficult) because most ources required for such an attactionally need online access to a tey that is shared between multip	e very difficult to perform of the work necessary to k would be very significan n unpatched system using ble clients. This only affec	and deduce nt and g the
VE-2016-8743	https://nvd.nist.gov/vu	2017-07-27	208.11.141.88	80	2019-01-
	In/detail/CVE-2016- 8743		200.11.141.00		06T12:13:29.238Z
nes and headers. Acce teracts with back-end		epresented a security	ne whitespace accepted from re concern when httpd participate	s in any chain of proxies	nse or
pache HTTP Server, ir nes and headers. Acce teracts with back-end	8743 all releases prior to 2.2.32 and application servers, either through	epresented a security	ne whitespace accepted from re concern when httpd participate	s in any chain of proxies	nse or
pache HTTP Server, in nes and headers. Acce teracts with back-end muggling, response sp VE-2015-3183 escription: ne chunked transfer comote attackers to cor	a all releases prior to 2.2.32 and a epting these different behaviors rapplication servers, either through litting and cache pollution. https://nvd.nist.gov/vuln/detail/CVE-2015-	epresented a security gh mod_proxy or using 2015-07-20 che HTTP Server befotacks via a crafted req	ne whitespace accepted from re concern when httpd participate g conventional CGI mechanisms 208.11.141.88	s in any chain of proxies is, and may result in requests 80	2019-01- 06T12:13:29.238Z
pache HTTP Server, in nes and headers. Acce teracts with back-end muggling, response sp VE-2015-3183 escription: ne chunked transfer comote attackers to cor	all releases prior to 2.2.32 and appling these different behaviors rapplication servers, either through the servers of the ser	epresented a security gh mod_proxy or using 2015-07-20 che HTTP Server befotacks via a crafted req	ne whitespace accepted from re concern when httpd participate g conventional CGI mechanisms 208.11.141.88	s in any chain of proxies is, and may result in requests 80	2019-01- 06T12:13:29.238Z
pache HTTP Server, in less and headers. Acce teracts with back-end muggling, response spokes. VE-2015-3183 escription: The chunked transfer commote attackers to convalid chunk-extension vE-2015-3185 escription: The less applicable application in less application i	a all releases prior to 2.2.32 and a epting these different behaviors rapplication servers, either through the prior of th	epresented a security gh mod_proxy or using 2015-07-20 che HTTP Server befotacks via a crafted requiliters.c. 2015-07-20 c in the Apache HTTP grather than an auther	ne whitespace accepted from reconcern when httpd participate g conventional CGI mechanisms 208.11.141.88 The 2.4.14 does not properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, and the properly parsquest to the properly parsquest	s in any chain of proxies is, and may result in requests, and may result in requests and see chunk headers, which a large chunk-size values at 80	2019-01- 06T12:13:29.238Z allows and 2019-01- 06T07:21:26.017Z
pache HTTP Server, in less and headers. Acce teracts with back-end muggling, response spokes. VE-2015-3183 escription: The chunked transfer commote attackers to convalid chunk-extension vE-2015-3185 escription: The less applicable application in less application i	all releases prior to 2.2.32 and appling these different behaviors of application servers, either through litting and cache pollution. https://nvd.nist.gov/vu ln/detail/CVE-2015-3183 adding implementation in the Aparduct HTTP request smuggling at characters in modules/http/http. https://nvd.nist.gov/vu ln/detail/CVE-2015-3185	epresented a security gh mod_proxy or using 2015-07-20 che HTTP Server befotacks via a crafted requiliters.c. 2015-07-20 c in the Apache HTTP grather than an auther	ne whitespace accepted from reconcern when httpd participate g conventional CGI mechanisms 208.11.141.88 The 2.4.14 does not properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, related to mishandling of Incomparent to the properly parsquest, and the properly parsquest to the properly parsquest	s in any chain of proxies is, and may result in requests, and may result in requests and see chunk headers, which a large chunk-size values at 80	2019-01- 06T12:13:29.238Z allows and 2019-01- 06T07:21:26.017Z

CVE-2017-3736					
	https://nvd.nist.gov/vu In/detail/CVE-2017-	2017-11-02	208.11.141.177	80	2019-01- 06T07:21:26.017Z
algorithms are affected. are not believed likely. A information about a privalikely only accessible to target private key in a sc	3736 ting bug in the x86_64 Montgor Analysis suggests that attacks a ttacks against DH are considere ate key may be performed offline a limited number of attackers. A renario with persistent DH paran the BMI1, BMI2 and ADX extens	gainst RSA and DSA as a re ed just feasible (although ve e. The amount of resources n attacker would additional neters and a private key tha	esult of this defect would be ery difficult) because most of required for such an attack ly need online access to an at is shared between multiple	very difficult to perform and the work necessary to deduce would be very significant and unpatched system using the e clients. This only affects	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	208.11.141.177	80	2019-01- 06T07:21:26.017Z
remote attackers to cond	ding implementation in the Apaduct HTTP request smuggling at characters in modules/http/http_	tacks via a crafted request,			
CVE-2017-3738	https://nvd.nist.gov/vu In/detail/CVE-2017- 3738	2017-12-07	208.11.141.177	80	2019-01- 06T07:21:26.017Z
are affected. Analysis subelieved likely. Attacks a private key may be perfc TLS to be meaningful, th 2016-0701. This only affe from this issue is similar Fixed in OpenSSL 1.0.2n	g in the AVX2 Montgomery multi ggests that attacks against RSA gainst DH1024 are considered j ormed offline. The amount of res e server would have to share th acts processors that support the to CVE-2017-3736, CVE-2017-37 Due to the low severity of this Oh when it becomes available. I	and DSA as a result of this just feasible, because most sources required for such ar e DH1024 private key amor AVX2 but not ADX extensions and CVE-2015-3193. Opissue we are not issuing a not such as the such as	defect would be very difficution of the work necessary to den attack would be significant ing multiple clients, which is roons like Intel Haswell (4th genenSSL version 1.0.2-1.0.2m are release of OpenSSL 1.1.0	If to perform and are not educe information about a t. However, for an attack on no longer an option since CVE-eneration). Note: The impact and 1.1.0-1.1.0g are affected.	
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	208.11.141.177	80	2019-01- 06T07:21:26.017Z
(heap-based buffer overlimproper scoreboard had	od_status module in the Apache flow), or possibly obtain sensitiv nodling within the status_handler	e credential information or e	execute arbitrary code, via a	crafted request that triggers	
iuriction in modules/lua/l	lua_request.c.				
function in modules/lua/l	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	208.11.141.177	80	2019-01- 06T07:21:26.017Z
Description: OpenSSL 1.0.2 (starting f handshake then OpenSS as designed for the expli work correctly if SSL_rea initial function call. If SSL is passed without being have to be present that r	https://nvd.nist.gov/vu In/detail/CVE-2017-	an "error state" mechanism. Ite and would immediately f o_handshake(), SSL_accep Itly. In that scenario, if the ha rily called by the applicatio om the SSL/TLS record layer ISL_write() being issued afte	The intent was that if a fatal rail if you attempted to continut to and SSL_connect()), howe and shake fails then a fatal ern for the same SSL object the r. In order to exploit this issu	error occurred during a nue the handshake. This works ever due to a bug it does not rror will be returned in the nen it will succeed and the data te an application bug would	
Description: OpenSSL 1.0.2 (starting f handshake then OpenSS as designed for the expli work correctly if SSL_rea initial function call. If SSL is passed without being have to be present that r 1.0.2b-1.0.2m are affected.	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737 from version 1.0.2b) introduced a SL would move into the error sta- icit handshake functions (SSL_d ad() or SSL_write() is called direc- _read()/SSL_write() is subseque decrypted/encrypted directly for resulted in a call to SSL_read()/S	an "error state" mechanism. Ite and would immediately f o_handshake(), SSL_accep Itly. In that scenario, if the ha rily called by the applicatio om the SSL/TLS record layer ISL_write() being issued afte	The intent was that if a fatal rail if you attempted to continut to and SSL_connect()), howe and shake fails then a fatal ern for the same SSL object the r. In order to exploit this issu	error occurred during a nue the handshake. This works ever due to a bug it does not rror will be returned in the nen it will succeed and the data te an application bug would	
Description: OpenSSL 1.0.2 (starting f handshake then OpenSS as designed for the expli work correctly if SSL_readinitial function call. If SSL is passed without being have to be present that in 1.0.2b-1.0.2m are affected. CVE-2015-3183 Description: The chunked transfer coremote attackers to concern.	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737 from version 1.0.2b) introduced a SL would move into the error sta icit handshake functions (SSL_d ad() or SSL_write() is called direcread()/SSL_write() is subseque decrypted/encrypted directly fro resulted in a call to SSL_read()/S d. Fixed in OpenSSL 1.0.2n. Ope https://nvd.nist.gov/vu In/detail/CVE-2015-	an "error state" mechanism. tte and would immediately f o_handshake(), SSL_accep tity. In that scenario, if the ha ntly called by the applicatio om the SSL/TLS record layer SSL_write() being issued after enSSL 1.1.0 is not affected. 2015-07-20 che HTTP Server before 2.4 ttacks via a crafted request,	The intent was that if a fatal fail if you attempted to contint (t) and SSL_connect()), howe andshake fails then a fatal e in for the same SSL object the forth or the same standard the same standard fails the same standard fails and same	error occurred during a nue the handshake. This works ever due to a bug it does not rror will be returned in the nen it will succeed and the data te an application bug would fatal error. OpenSSL version 80 chunk headers, which allows	06T07:21:26.017Z

The spis someand. required function in surrestroques is in the Apache HTTP Server 2.4.s. before 2.4.4 dicase not consider that a Require directive may be associated with an administration settler, without assess restrictions in opportunistic circumstances. by incompany the presence of a module that relate on the 2.2.48 behavior. CVE-2016-0703 Indicatal/CVE-2016-0703 Indicatal/CVE-2016-0703 Description: The get_chent_master_key function in s2_svvr c in the SSLv2 implementation in OpenSSL before 0.9.8rt, 10.0 before 10.0r, 10.1 before 10.0r, 10.1 before 10.0r, and 10.2 before 10.22 accepts a resource CLERT MASTER KEY CLEAR KEY LEAST that the interest on the same state of the service and decays 11.5 cepturities tools by teveraging of Biochembecher SSA predified oncice, a related issue to CVE-2016-0300. CVE-2016-3195 https://mvd.nist.gov/vu 2015-12-06 20.8.11.11.155 80 2019-01-06704.21.43.905.Z Description: The SRIT THG. COMBNE implementation in opportunistical Nature does by teveraging of Biochembecher SSA predified in the service of the servic		In/detail/CVE-2015-				06T04:21:43.905Z
The registering control is required function in surrectinguate in the Apacher ITTP Server 2.4 is before 2.4.4 shees not candide that is Require interview in the Server interview and the Server int		3185				
Description: The get_Clein_Timoster_New function in \$2_sext_c in the SSLV2 implementation in OpenSSL before 0.9 8xf, 1.0.0 before 1.0.0r, 1.01 before The get_Clein_Timoster_New function in \$2_sext_c in the SSLV2 implementation in OpenSSL before 0.9 8xf, 1.0.0 before 1.0.0r, 1.01 before The get_Clein_Timoster_New function in \$2_sext_c in the SSLV2 implementation in OpenSSL before 0.9 8xf, 1.0.0 before 1.0.0r, 1.01 before The SELVE CLEIN_TIMOstory of the SELVE CLEIN_TIMOstric Value for an intrinsip clein of the SELVE CLEIN_TIMOstric Value for an intrinsip clein of the SELVE CLEIN_TIMOstric Value for an intrinsip clein of the SELVE CLEIN_TIMOstric Value for an intrinsip clein of the SELVE CLEIN_TIMOstric Value for an intrinsip clein of the SELVE CLEIN_TIMOstric Value for an intrinsip clein of the SELVE CLEIN_TIMOstric Value for an intrinsip clein of the SELVE CLEIN_TIMOstric Value for an intrinsip clein of the SELVE CLEIN_TIMOstric Value for an intrinsip clein of the SELVE CLEIN_TIMOstric Value for an intrinsip clein of the SELVE CLEIN_TIMOstric Value for an intrinsip clein of the SELVE CLEIN CLE	directive may be associat	ted with an authorization setting	g rather than an authenticatio	n setting, which allows remot	e attackers to bypass	
The get_client_master_key function in \$2_styr.c in the SSL2 implementation in OpenSSL before 0.9 Set, 10.0 before 10.0 in, cold 1.0 before 10.0 in, and 10.2 before 10.20 accepts an anotaron CLIENT-MASTER-KEY CLEAR KEY-LENDRY that for an arbitrary opiner, which allows manned the mode statistics to determine the MASTER-KEY value and decryst TLS ciphertext data by leveraging a Biechenbacher RSA padding words, a related is sub to VEX-2076-6 but of VEX-2076-6 but	CVE-2016-0703	In/detail/CVE-2016-	2016-03-02	208.11.141.155	80	
In/detail/CVE-2015-3195 Description: The ASNLTRLG_COMBINE implementation in cryptolastitians. decc in OpenSSL before 0.9.8th, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.tt, and 1.0.2 before 1.0.2 emishandles errors caused by mailtamed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application. CVE-2016-8743 https://mvd.nist.gov/vu 2017-07-27 208.11.141.155 80 2019-01-017-017-017-017-017-017-017-017-017-	1.0.1m, and 1.0.2 before 1. in-the-middle attackers to	0.2a accepts a nonzero CLIEN odetermine the MASTER-KEY v	Γ-MASTER-KEY CLEAR-KEY-L	ENGTH value for an arbitrary	cipher, which allows man-	
The ASNL TFLG_COMBINE implementation in crypto/asnlanas, dec.c in OpenSSL before 0.9 s8zh, 1.0.0 before 1.0.0t, 1.0 thefore 1.0.1t, and 1.0.2 before 1.0.2th embandles errors caused by mildinemate X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS97 or CMS application. CVE-2016-8743 https://ruxd.nist.gov/vu Indicatali/CVE-2016-8743 ltd; indicatali/CVE-2016-8743 bttps://ruxd.nist.gov/vu Indicatali/CVE-2016-8743 bttps://ruxd.nist.gov/vu Indicatali/CVE-2016-8743 bttps://ruxd.nist.gov/vu Indicatali/CVE-2016-8743 bttps://ruxd.nist.gov/vu Indicatali/CVE-2016-8743 bttps://ruxd.nist.gov/vu Indicatali/CVE-2016-8743 bttps://ruxd.nist.gov/vu Indicatali/CVE-2014-926 bttps://ruxd.nist.gov/vu Indicatali/CVE-2015-3194 bttps://ruxd.nist.gov/vu Indicatali/CVE-2015-3194 bttps://ruxd.nist.gov/vu Indicatali/CVE-2015-3194 bttps://ruxd.nist.gov/vu Indicatali/CVE-2015-3194 bttps://ruxd.nist.gov/vu Indicatali/CVE-2015-3194 bttps://ruxd.nist.gov/vu Indicatali/CVE-2015-3194 bttps://ruxd.nist.gov/vu Indicatali/CVE-2015-3197 bttps://ruxd.nist.gov/vu Indicatali/CVE-2015-3197 bttps://ruxd.nist.gov/vu Indicatali/CVE-2015-3197 bttps://ruxd.nist.gov/vu Indicatali/CVE-2015-3197 bttps://ruxd.nist.gov/vu Indicatali/CVE-2016-9800 bttps://ruxd.nist.gov/vu Indicatali/CVE-2016-	CVE-2015-3195	In/detail/CVE-2015-	2015-12-06	208.11.141.155	80	
In/detail/CVE-2016-8743 Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when intigh participates in any chain of proxise or interacts with backend application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution. CVE-2014-0226 https://nvd.nist.gov/vu ln/detail/CVE-2014-0226 https://nvd.nist.gov/vu ln/detail/CVE-2014-0226 https://nvd.nist.gov/vu ln/detail/CVE-2014-0226 https://nvd.nist.gov/vu ln/detail/CVE-2014-0226 https://nvd.nist.gov/vu ln/detail/CVE-2014-0226 https://nvd.nist.gov/vu ln/detail/CVE-2015-1026 https://nvd.nist.gov/vu ln/detail/CVE-2015-1026 https://nvd.nist.gov/vu ln/detail/CVE-2015-1039 https://nvd.nist.gov/vu ln/detail/CVE-2015-10394 https://nvd.nist.gov/vu ln/detail/CVE-2016-10394 https://nvd.nist.gov/vu ln/detail/CVE-2016-10394 https://nvd.nist.gov/v	1.0.2 before 1.0.2e mishar	ndles errors caused by malform	ied X509_ATTRIBUTE data, v	which allows remote attackers		
Apache HTTP Server, in all releases prior to 2.3.2 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors representatives a security concern when httpd participates in any chain of proxise or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution. CVE-2014-0226	CVE-2016-8743	In/detail/CVE-2016-	2017-07-27	208.11.141.155	80	
In/detail/CVE-2014- 0226 Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_sp_scoreboard_worker function in modules/lua/fua_request.c CVE-2015-3194 https://nvd.nist.gov/vu 2015-12-06 208.11.141.155 80 2019-01- In/detail/CVE-2015- 3194 https://nvd.nist.gov/vu 2015-12-06 208.11.141.155 80 2019-01- Description: crypto//sa/rsa_ameth.c in OpenSSL 1.0.1 before 10.1q and 10.2 before 10.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter. CVE-2015-3197 https://nvd.nist.gov/vu 2016-02-14 208.11.141.155 80 2019-01- Un/detail/CVE-2015-3197 https://nvd.nist.gov/vu 2016-02-14 208.11.141.155 80 2019-01- O6T04:21:43.905Z Description: ssl/s2_svr.c in OpenSSL 1.0.1 before 1.0.tr and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in- the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_hello functions. CVE-2016-0800 https://nvd.nist.gov/vu 2016-03-01 63.128.95.117 443 2019-01- Un/detail/CVE-2016- 0800 Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS	lines and headers. Accep interacts with back-end a	iting these different behaviors r pplication servers, either throug	epresented a security concer	rn when httpd participates in a	any chain of proxies or	
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c. CVE-2015-3194	CVE-2014-0226	In/detail/CVE-2014-	2014-07-20	208.11.141.155	80	
In/detail/CVE-2015-3194 Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter. CVE-2015-3197 https://nvd.nist.gov/vu 2016-02-14 208.11.141.155 80 2019-01- 06T04:21:43.905Z 3197 Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions. CVE-2016-0800 https://nvd.nist.gov/vu 2016-03-01 63.128.95.117 443 2019-01- 02T14:22:27.811Z Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS	(heap-based buffer overflimproper scoreboard han	low), or possibly obtain sensitive adding within the status_handler	e credential information or ex	ecute arbitrary code, via a cra	afted request that triggers	
crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter. CVE-2015-3197 https://nvd.nist.gov/vu 2016-02-14 208.11.141.155 80 2019-01-	CVE-2015-3194	In/detail/CVE-2015-	2015-12-06	208.11.141.155	80	
In/detail/CVE-2015- 3197 Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions. CVE-2016-0800 https://nvd.nist.gov/vu 2016-03-01 63.128.95.117 443 2019-01- In/detail/CVE-2016- 0800 Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS						
ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions. CVE-2016-0800 https://nvd.nist.gov/vu 2016-03-01 63.128.95.117 443 2019-01- In/detail/CVE-2016- 0800 02T14:22:27.811Z Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS	CVE-2015-3197	In/detail/CVE-2015-	2016-02-14	208.11.141.155	80	
In/detail/CVE-2016- 0800 Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS	the-middle attackers to de	efeat cryptographic protection				
The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS	CVE-2016-0800	In/detail/CVE-2016-	2016-03-01	63.128.95.117	443	
	message before establish	ning that a client possesses cer	tain plaintext RSA data, which	n makes it easier for remote a		

Conception:						
consecution for the CBMD 9 is before 9.93.8 P4 and 9.0 is before 9.03.8 P4 and 9.0 is before 9.0 in the Composition of the CBMD of the CBM	CVE-2016-1286	In/detail/CVE-2016-	2016-03-09	64.149.172.30	53	
Description: SC BIND through 9.9.9-Pt 3.10x through 9.10-Pt and 9.11x through 9.11x thro	named in ISC BIND 9.x bef				rvice (assertion failure and	
ISC BIND through 9.9 Pt. 9.10.th through 9.9 Pt. 9.10.th windows and allows primary DNS services to cause a denial of service (partial via a large UPDATE monosping). CVE-2016-8864	CVE-2016-6170	In/detail/CVE-2016-	2016-07-06	64.149.172.30	53	
Description: Invide tail/CVE-2016- Security Sec	ISC BIND through 9.9.9-P1, (secondary DNS server cra a large IXFR response and	sh) via a large AXFR response	e, and possibly allows IXFR se	ervers to cause a denial of se	vice (IXFR client crash) via	
named in ISC BIND 9 x before 9 9.9-P4, 9.10 x before 9 10.4-P4, and 9.11x before 9.110-P1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a DNAME record in the answer section of a response to a recursive query, related to db. c and resolver. CVE-2016-1285	CVE-2016-8864	In/detail/CVE-2016-	2016-11-02	64.149.172.30	53	
In/detail/CVE-2016- 1285	named in ISC BIND 9.x bef (assertion failure and daem					
named in ISC BIND 9 x before 9 9.8-P4 and 9.10 x before 9.10 3-P4 does not properly handle DNAME records when parsing fetch reply messages, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed packet to the rinde (aka control channel) interface, related to alist c and sexpr.c. CVE-2016-9444	CVE-2016-1285	In/detail/CVE-2016-	2016-03-09	64.149.172.30	53	
In/detail/CVE-2016-9444 Description: named in ISC BIND 9 x before 9.9.9-9-P5, 9.10 x before 9.10.4-P5, and 9.11 x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted DS resource record in an answer. CVE-2015-8704	named in ISC BIND 9.x bef messages, which allows re	mote attackers to cause a de	nial of service (assertion failu			
named in ISC BIND 9.x before 9.9.9-P.5, 9.10 x before 9.10.4-P.5, and 9.11 x before 9.11.0-P.2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted DS resource record in an answer. CVE-2015-8704	CVE-2016-9444	In/detail/CVE-2016-	2017-01-12	64.149.172.30	53	
In/detail/CVE-2015-8704 Description: apL_42.c in ISC BIND 9.x before 9.9.8-P3, 9.9.x, and 9.10.x before 9.10.3-P3 allows remote authenticated users to cause a denial of service (INSIST assertion failure and daemon exit) via a malformed Address Prefix List (APL) record. CVE-2016-9131	named in ISC BIND 9.x bef	•	•		to cause a denial of	
apl_42.c in ISC BIND 9.x before 9.9.8-P3, 9.9.x, and 9.10.x before 9.10.3-P3 allows remote authenticated users to cause a denial of service (INSIST assertion failure and daemon exit) via a malformed Address Prefix List (APL) record. CVE-2016-9131	CVE-2015-8704	In/detail/CVE-2015-	2016-01-20	64.149.172.30	53	
Description: named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed response to an RTYPE ANY query. CVE-2015-8000 https://nvd.nist.gov/vu 2015-12-16 64.149.172.30 53 2019-01- 01T15:31:06.385Z Description: db.c in named in ISC BIND 9.x before 9.9.8-P2 and 9.10.x before 9.10.3-P2 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via a malformed class attribute.	apl_42.c in ISC BIND 9.x be				ause a denial of service	
named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed response to an RTYPE ANY query. CVE-2015-8000 https://nvd.nist.gov/vu 2015-12-16 64.149.172.30 53 2019-01- In/detail/CVE-2015- 8000 Description: db.c in named in ISC BIND 9.x before 9.9.8-P2 and 9.10.x before 9.10.3-P2 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via a malformed class attribute.	CVE-2016-9131	In/detail/CVE-2016-	2017-01-12	64.149.172.30	53	
In/detail/CVE-2015-8000 Description: db.c in named in ISC BIND 9.x before 9.9.8-P2 and 9.10.x before 9.10.3-P2 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via a malformed class attribute.	named in ISC BIND 9.x bef				to cause a denial of	
db.c in named in ISC BIND 9.x before 9.9.8-P2 and 9.10.x before 9.10.3-P2 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via a malformed class attribute.	CVE-2015-8000	In/detail/CVE-2015-	2015-12-16	64.149.172.30	53	
CVE-2016-0800 https://nvd.nist.gov/vu 2016-03-01 50.58.10.133 443 2019-01-	db.c in named in ISC BIND			note attackers to cause a deni	al of service (REQUIRE	
	CVE-2016-0800	https://nvd.nist.gov/vu	2016-03-01	50.58.10.133	443	2019-01-

	In/detail/CVE-2016- 0800				01T13:10:54.409Z
nessage before establishi		tain plaintext RSA data, whi	ther products, requires a serve ch makes it easier for remote a l" attack.		
CVE-2017-3736	https://nvd.nist.gov/vu In/detail/CVE-2017- 3736	2017-11-02	166.73.13.9	443	2018-12- 29T15:37:33.193Z
algorithms are affected. Ar are not believed likely. Atta nformation about a private ikely only accessible to a l arget private key in a scer	nalysis suggests that attacks a acks against DH are considers e key may be performed offlin limited number of attackers. A nario with persistent DH paran	gainst RSA and DSA as a re ed just feasible (although ve e. The amount of resources n attacker would additionall neters and a private key tha	OpenSSL before 1.0.2m and 1. sult of this defect would be very difficult) because most of the required for such an attack way need online access to an unit is shared between multiple of a generation) and later or AMD	ry difficult to perform and e work necessary to deduce ould be very significant and patched system using the lients. This only affects	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	166.73.13.9	443	2018-12- 29T15:37:33.193Z
ines and headers. Accepti	ing these different behaviors replication servers, either through	epresented a security conc	itespace accepted from reque ern when httpd participates in ventional CGI mechanisms, and	any chain of proxies or	
CVE-2017-3738	https://nvd.nist.gov/vu In/detail/CVE-2017- 3738	2017-12-07	166.73.13.9	443	2018-12- 29T15:37:33.193Z
are affected. Analysis suggesteleved likely. Attacks again and the perform LS to be meaningful, the 2016-0701. This only affect from this issue is similar to Fixed in OpenSSL 1.0.2n. E	gests that attacks against RSA ainst DH1024 are considered j med offline. The amount of res server would have to share th ts processors that support the CVE-2017-3736, CVE-2017-37 Due to the low severity of this	and DSA as a result of this ust feasible, because most sources required for such ar e DH1024 private key amon AVX2 but not ADX extensions and CVE-2015-3193. Options we are not issuing a new AVX2 we are not issuing a new AVX2 when is the control of the control o	exponentiation with 1024-bit r defect would be very difficult to of the work necessary to dedu attack would be significant. H g multiple clients, which is no ons like Intel Haswell (4th gene enSSL version 1.0.2-1.0.2m and ew release of OpenSSL 1.1.0 at mmit e502cc86d in the OpenS	o perform and are not ice information about a lowever, for an attack on longer an option since CVE-pration). Note: The impact of 1.1.0-1.1.0g are affected. It this time. The fix will be	
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	166.73.13.9	443	2018-12- 29T15:37:33.193Z
lirective may be associate	ed with an authorization setting	g rather than an authenticati	er 2.4.x before 2.4.14 does not on setting, which allows remot nce of a module that relies on	te attackers to bypass	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	166.73.13.9	443	2018-12- 29T15:37:33.193Z
emote attackers to condu	3	tacks via a crafted request,	.14 does not properly parse ch related to mishandling of large	•	
CVE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	166.73.13.9	443	2018-12- 29T15:37:33.193Z
Description: OpenSSL 1.0.2 (starting fro	om version 1.0.2b) introduced a	an "error state" mechanism.	The intent was that if a fatal er	ror occurred during a	

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the

is passed without being de have to be present that res	ead()/SSL_write() is subseque crypted/encrypted directly fro sulted in a call to SSL_read()/S Fixed in OpenSSL 1.0.2n. Ope	om the SSL/TLS record layer. SSL_write() being issued after	In order to exploit this issue a	n application bug would			
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	166.73.13.9	443	2018-12- 29T15:37:33.193Z		
(heap-based buffer overflo	_status module in the Apache w), or possibly obtain sensitiv ling within the status_handler _request.c.	e credential information or ex	ecute arbitrary code, via a cra	afted request that triggers			
CVE-2015-3195	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	208.11.141.73	443	2018-12- 29T15:04:59.465Z		
1.0.2 before 1.0.2e mishand	E implementation in crypto/as dles errors caused by malform nemory by triggering a decod	ned X509_ATTRIBUTE data, v	which allows remote attackers				
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	208.11.141.73	443	2018-12- 29T15:04:59.465Z		
directive may be associate	ed function in server/request. d with an authorization setting is in opportunistic circumstand	g rather than an authenticatio	n setting, which allows remote	e attackers to bypass			
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	208.11.141.73	443	2018-12- 29T15:04:59.465Z		
(heap-based buffer overflo	_status module in the Apache w), or possibly obtain sensitiv ling within the status_handler _request.c.	e credential information or ex	ecute arbitrary code, via a cra	afted request that triggers			
CVE-2015-3197	https://nvd.nist.gov/vu In/detail/CVE-2015- 3197	2016-02-14	208.11.141.73	443	2018-12- 29T15:04:59.465Z		
the-middle attackers to def	0.1 before 1.0.1r and 1.0.2 before tryptographic protection d get_client_hello functions.						
CVE-2016-0703	https://nvd.nist.gov/vu ln/detail/CVE-2016- 0703	2016-03-02	208.11.141.73	443	2018-12- 29T15:04:59.465Z		
1.0.1m, and 1.0.2 before 1.0. in-the-middle attackers to d	Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows manin-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.						
CVE-2015-3194	https://nvd.nist.gov/vu In/detail/CVE-2015- 3194	2015-12-06	208.11.141.73	443	2018-12- 29T15:04:59.465Z		
	OpenSSL 1.0.1 before 1.0.1q an oplication crash) via an RSA P			•			
CVE-2015-3183	https://nvd.nist.gov/vu	2015-07-20	208.11.141.73	443	2018-12-		

Description: The chunked transfer coding in remote attackers to conduct HT invalid chunk-extension characters. CVE-2016-8743 ht In., 87 Description: Apache HTTP Server, in all relelines and headers. Accepting the	TTP request smuggling atta- ters in modules/http/http_f tttps://nvd.nist.gov/vu //detail/CVE-2016- 743 eases prior to 2.2.32 and 2. hese different behaviors re ation servers, either through and cache pollution.	acks via a crafted request, rel filters.c. 2017-07-27 4.25, was liberal in the white-presented a security concern	lated to mishandling of large of 208.11.141.73 space accepted from request		29T15:04:59.465Z 2018-12- 29T15:04:59.465Z
The chunked transfer coding in remote attackers to conduct HT invalid chunk-extension characters. CVE-2016-8743 ht In. 87 Description: Apache HTTP Server, in all rele lines and headers. Accepting the	TTP request smuggling atta- ters in modules/http/http_f tttps://nvd.nist.gov/vu //detail/CVE-2016- 743 eases prior to 2.2.32 and 2. hese different behaviors re ation servers, either through and cache pollution.	acks via a crafted request, rel filters.c. 2017-07-27 4.25, was liberal in the white-presented a security concern	lated to mishandling of large of 208.11.141.73 space accepted from request	chunk-size values and	
In, 87 Description: Apache HTTP Server, in all rele lines and headers. Accepting th	h/detail/CVE-2016- 743 eases prior to 2.2.32 and 2. hese different behaviors re ation servers, either through and cache pollution.	4.25, was liberal in the white presented a security concern	space accepted from request	443	
Apache HTTP Server, in all rele lines and headers. Accepting th	hese different behaviors re ation servers, either through and cache pollution.	presented a security concern			
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
In	n/detail/CVE-2016- 743	2017-07-27	208.11.141.92	443	2018-12- 29T08:51:43.537Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
In	ttps://nvd.nist.gov/vu n/detail/CVE-2015- 185	2015-07-20	208.11.141.92	443	2018-12- 29T08:51:43.537Z
Description: The ap_some_auth_required fu directive may be associated wit intended access restrictions in	th an authorization setting	rather than an authentication	setting, which allows remote	attackers to bypass	
In	ttps://nvd.nist.gov/vu n/detail/CVE-2014- 226	2014-07-20	208.11.141.92	443	2018-12- 29T08:51:43.537Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers mproper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
In	ttps://nvd.nist.gov/vu n/detail/CVE-2015- 183	2015-07-20	208.11.141.92	443	2018-12- 29T08:51:43.537Z
Description: The chunked transfer coding in remote attackers to conduct H1 invalid chunk-extension charact	TTP request smuggling atta	acks via a crafted request, rel			
In	ttps://nvd.nist.gov/vu //detail/CVE-2017- 738	2017-12-07	208.11.141.92	443	2018-12- 29T08:51:43.537Z
Description: There is an overflow bug in the are affected. Analysis suggests believed likely. Attacks against private key may be performed or TLS to be meaningful, the serve 2016-0701. This only affects profrom this issue is similar to CVE Fixed in OpenSSL 1.0.2n, Due to included in OpenSSL 1.1.0h when	s that attacks against RSA as DH1024 are considered ju offline. The amount of reso er would have to share the occssors that support the As-2017-3736, CVE-2017-3736 to the low severity of this is	and DSA as a result of this de- ist feasible, because most of i surces required for such an at DH1024 private key among i AVX2 but not ADX extensions 32 and CVE-2015-3193. Open: isue we are not issuing a new	fect would be very difficult to the work necessary to deduc ttack would be significant. Ho multiple clients, which is no lo s like Intel Haswell (4th general SSL version 1.0.2-1.0.2m and a verelease of OpenSSL 1.1.0 at t	perform and are not e information about a wever, for an attack on onger an option since CVE- ation). Note: The impact 1.1.0-1.1.0g are affected. this time. The fix will be	
	ttps://nvd.nist.gov/vu ı/detail/CVE-2017-	2017-11-02	208.11.141.92	443	2018-12- 29T08:51:43.537Z

3736

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2017-3737

https://nvd.nist.gov/vu 2017-12-07

208.11.141.92

443

2018-12-29T08:51:43.537Z

3737

In/detail/CVE-2017-

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2017-3737

https://nvd.nist.gov/vu 2017-12-07

192.131.76.23

443

2018-12-29T08:40:33.390Z

In/detail/CVE-2017-3737

Description

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the intention call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2015-3185

https://nvd.nist.gov/vu 2015-07-20 In/detail/CVE-2015192.131.76.23

443

2018-12-

29T08:40:33.390Z

3185

Description

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2017-3738

https://nvd.nist.gov/vu 2017-12-07 In/detail/CVE-2017192.131.76.23

443

2018-12-

29T08:40:33.390Z

3738

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0 hwhen it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2015-3183

https://nvd.nist.gov/vu In/detail/CVE-20152015-07-20

192.131.76.23

443

2018-12-29T08:40:33.390Z

3183

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2017-3736

https://nvd.nist.gov/vu In/detail/CVE-20172017-11-02

192.131.76.23

443

2018-12-

29T08:40:33.390Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HADWARE OR DARDWARE OR HADWARE OR HA

3736

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2014-0226

https://nvd.nist.gov/vu In/detail/CVE-20142014-07-20

192.131.76.23

443

2018-12-29T08:40:33.390Z

0226

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2016-8743

https://nvd.nist.gov/vu

2017-07-27

192.131.76.23

443

2018-12-

In/detail/CVE-2016-

8743

8743

3185

3738

29T08:40:33.390Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2016-8743

https://nvd.nist.gov/vu In/detail/CVE-20162017-07-27

208.11.141.204

443

2018-12-

29T05:22:32.080Z

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3185

https://nvd.nist.gov/vu In/detail/CVE-20152015-07-20

208.11.141.204

443

2018-12-

29T05:22:32.080Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2017-3738

https://nvd.nist.gov/vu In/detail/CVE-20172017-12-07

208 11 141 204

443

2018-12-

29T05:22:32.080Z

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2014-0226

https://nvd.nist.gov/vu In/detail/CVE-20142014-07-20

208.11.141.204

443

2018-12-29T05:22:32.080Z

0226

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker

function in modules/lua/l	ua_request.c.				
CVE-2017-3736	https://nvd.nist.gov/vu In/detail/CVE-2017- 3736	2017-11-02	208.11.141.204	443	2018-12- 29T05:22:32.080Z
algorithms are affected. A are not believed likely. A information about a privalikely only accessible to a target private key in a sc	ting bug in the x86_64 Montgor Analysis suggests that attacks a ttacks against DH are considerent te key may be performed offlinal a limited number of attackers. A enario with persistent DH parant the BMI1, BMI2 and ADX extens	gainst RSA and DSA as a re ed just feasible (although ve e. The amount of resources n attacker would additional neters and a private key tha	esult of this defect would be very difficult) because most of the required for such an attack who were defined and the required for such an attack who have a such as the shared between multiple of the state of the requirement is shared between multiple of the shared between multiple of the state of the shared between multiple of the shared between the shared be	ery difficult to perform and ne work necessary to deduce ould be very significant and neatched system using the clients. This only affects	
CVE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	208.11.141.204	443	2018-12- 29T05:22:32.080Z
handshake then OpenSS as designed for the expli work correctly if SSL_rea initial function call. If SSL is passed without being have to be present that r	rom version 1.0.2b) introduced a SL would move into the error sta- cit handshake functions (SSL_d ad) or SSL_write() is called direc _read()/SSL_write() is subseque decrypted/encrypted directly fro esulted in a call to SSL_read()/S d. Fixed in OpenSSL 1.0.2n. Ope	te and would immediately fo_handshake(), SSL_accep ttly. In that scenario, if the h. ntly called by the applicatio om the SSL/TLS record laye SSL_write() being issued afte	ail if you attempted to continu t() and SSL_connect()), howeve andshake fails then a fatal erro n for the same SSL object the r. In order to exploit this issue	e the handshake. This works er due to a bug it does not or will be returned in the n it will succeed and the data an application bug would	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	208.11.141.204	443	2018-12- 29T05:22:32.080Z
remote attackers to cond	ding implementation in the Apa duct HTTP request smuggling at characters in modules/http/http_	tacks via a crafted request,			
CVE-2015-3195	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	208.11.141.64	443	2018-12- 28T21:53:03.792Z
1.0.2 before 1.0.2e misha	INE implementation in crypto/as indles errors caused by malform is memory by triggering a decod	ned X509_ATTRIBUTE data	, which allows remote attacke		
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	208.11.141.64	443	2018-12- 28T21:53:03.792Z
remote attackers to cond	ding implementation in the Apa duct HTTP request smuggling at characters in modules/http/http_	tacks via a crafted request,			
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	208.11.141.64	443	2018-12- 28T21:53:03.792Z
(heap-based buffer overf	nd_status module in the Apache flow), or possibly obtain sensitiv ndling within the status_handler ua_request.c.	e credential information or	execute arbitrary code, via a c	rafted request that triggers	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	208.11.141.64	443	2018-12- 28T21:53:03.792Z

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or

Description:

	application servers, either through thing and cache pollution.	gh mod_proxy or using conve	entional CGI mechanisms, and	d may result in request		
CVE-2015-3194	https://nvd.nist.gov/vu In/detail/CVE-2015- 3194	2015-12-06	208.11.141.64	443	2018-12- 28T21:53:03.792Z	
	n OpenSSL 1.0.1 before 1.0.1q an application crash) via an RSA P					
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	208.11.141.64	443	2018-12- 28T21:53:03.792Z	
directive may be associate	uired function in server/request. ted with an authorization setting ons in opportunistic circumstand	g rather than an authenticatio	on setting, which allows remot	e attackers to bypass		
CVE-2015-3197	https://nvd.nist.gov/vu In/detail/CVE-2015- 3197	2016-02-14	208.11.141.64	443	2018-12- 28T21:53:03.792Z	
the-middle attackers to d	1.0.1 before 1.0.1r and 1.0.2					
CVE-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	208.11.141.64	443	2018-12- 28T21:53:03.792Z	
1.0.1m, and 1.0.2 before 1.	rey function in s2_srvr.c in the S .0.2a accepts a nonzero CLIENT o determine the MASTER-KEY v CVE-2016-0800.	Γ-MASTER-KEY CLEAR-KEY-L	ENGTH value for an arbitrary	cipher, which allows man-		
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	166.73.6.220	443	2018-12- 17T01:25:40.000Z	
directive may be associa	uired function in server/request. ted with an authorization setting ons in opportunistic circumstand	g rather than an authenticatio	n setting, which allows remot	e attackers to bypass		
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	166.73.6.220	443	2018-12- 17T01:25:40.000Z	
lines and headers. Acceptinteracts with back-end a	all releases prior to 2.2.32 and 2 oting these different behaviors r application servers, either through titing and cache pollution.	epresented a security conce	rn when httpd participates in	any chain of proxies or		
CVE-2017-3738	https://nvd.nist.gov/vu In/detail/CVE-2017- 3738	2017-12-07	166.73.6.220	443	2018-12- 17T01:25:40.000Z	
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not policyed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be ncluded in OpenSSL 1.1.0 when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.						

CVE-2017-3736	https://nvd.nist.gov/vu In/detail/CVE-2017- 3736	2017-11-02	166.73.6.220	443	2018-12- 17T01:25:40.000Z
algorithms are affected. An are not believed likely. Atta information about a private likely only accessible to a I target private key in a scer	ng bug in the x86_64 Montgon halysis suggests that attacks a acks against DH are considere key may be performed offlin- imited number of attackers. A hario with persistent DH paran e BMI1, BMI2 and ADX extens	gainst RSA and DSA as a res ed just feasible (although very e. The amount of resources ro n attacker would additionally neters and a private key that	ult of this defect would be ver or difficult) because most of the equired for such an attack wo need online access to an ung s shared between multiple cli	ry difficult to perform and e work necessary to deduce uld be very significant and patched system using the ients. This only affects	
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	166.73.6.220	443	2018-12- 17T01:25:40.000Z
(heap-based buffer overflo	_status module in the Apache w), or possibly obtain sensitiv lling within the status_handler _request.c.	e credential information or ex	ecute arbitrary code, via a cra	afted request that triggers	
CVE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	166.73.6.220	443	2018-12- 17T01:25:40.000Z
handshake then OpenSSL as designed for the explicit work correctly if SSL_readl initial function call. If SSL_r is passed without being de have to be present that res	m version 1.0.2b) introduced a would move into the error state thandshake functions (SSL_d) or SSL_write() is called directed()/SSL_write() is subsequencrypted/encrypted directly frosulted in a call to SSL_read()/SFixed in OpenSSL 1.0.2n. Open	ite and would immediately fai o_handshake(), SSL_accept() ttly. In that scenario, if the har ntly called by the application om the SSL/TLS record layer. SSL_write() being issued after	I if you attempted to continue and SSL_connect()), however dshake fails then a fatal error for the same SSL object then In order to exploit this issue a	the handshake. This works r due to a bug it does not will be returned in the it will succeed and the data n application bug would	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	166.73.6.220	443	2018-12- 17T01:25:40.000Z
remote attackers to condu	ng implementation in the Apa ct HTTP request smuggling at aracters in modules/http/http_	tacks via a crafted request, re			

RECOMMENDATION

Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment. Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the Bugtraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular update schedule for all software and hardware in use within your organization, ensuring that all the latest patches are applied soon after they are released.

ABOUT THIS ISSUE

Common vulnerabilities and exposures (CVE) is a list of publicly-known vulnerabilities in software and hardware. Each CVE contains an ID, a description of the vulnerability, and the product names and versions which are affected by the vulnerability. Software and hardware frequently self-report their product name and version when hosts connect to them. By searching through the CVE list and cross-referencing the names and versions of products found on this company's network, we are able to infer the presence of vulnerabilities.

PATCHING CADENCE > ISSUE DETAIL

End-of-Life Product

We observed an end-of-life product, one that is no longer developed or sold, publicly exposed.

-0.4 SCORE

23 findings

PRODUCT NAME	PRODUCT VERSION	STATE EFFECTIVE DATE	STATE REF	LAST SEEN	
Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-08- 10T21:46:55.862Z	2019-01- 17T18:14:29.000Z
Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-08- 11T18:56:57.235Z	2019-01- 16T20:23:14.000Z
Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-10- 15T20:23:10.000Z	2019-01- 16T20:19:37.000Z
Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-08- 04T12:22:22.792Z	2019-01- 10T07:25:23.000Z
Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-10- 21T17:24:49.161Z	2018-12- 29T18:10:03.589Z
Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-08- 11T17:41:11.425Z	2018-12- 29T16:41:07.480Z
Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-08- 11T00:17:30.776Z	2018-12- 29T16:15:55.619Z
Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-08- 11T08:02:29.916Z	2018-12- 29T15:39:00.441Z
Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-10- 21T19:03:57.396Z	2018-12- 29T13:47:37.321Z
Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-08- 10T21:41:14.013Z	2018-12- 29T11:13:17.297Z
Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-10- 22T12:24:39.265Z	2018-12- 29T11:00:26.011Z
Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-10- 21T21:49:32.979Z	2018-12- 29T08:11:04.169Z
	Internet Information Services 7.0 Internet Information Services 7.0	Internet Information Services 7.0 Internet Information Services 7.0	Internet Information Services 7.0 Internet Information Services 7.0	Internet	Internet Information Services 7.0

Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-08- 11T02:04:58.648Z	2018-12- 29T07:38:03.735Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-08- 11T04:27:54.419Z	2018-12- 29T06:03:07.310Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-10- 22T12:26:22.174Z	2018-12- 29T04:40:30.253 Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-12- 29T04:18:57.703Z	2018-12- 29T04:18:57.703Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-12- 29T03:39:08.542 Z	2018-12- 29T03:39:08.542 Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-08- 11T13:40:31.260Z	2018-12- 28T23:36:23.908Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-08- 11T01:00:58.279Z	2018-12- 28T23:12:54.531Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-08- 11T02:06:08.110Z	2018-12- 28T21:26:34.557Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-09- 15T12:55:23.295Z	2018-12- 28T21:04:52.428Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-08- 11T06:41:41.232Z	2018-12- 28T20:36:11.305Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.mic rosoft.com/en- us/lifecycle? p1=12925	2018-10- 22T00:46:02.283 Z	2018-12- 28T20:35:01.625Z

RECOMMENDATION

Ensure the affected product has an extended support contract that includes security patches. Review the vendor's statement of EOL guidelines for replacement products and upgrade to a new product line or manufacturer.

ABOUT THIS ISSUE

A product that has been declared as end-of-life (EOL) by the manufacturer has been detected. An EOL product is no longer marketed, sold, or upgraded by the manufacturer. Products at this stage in their life cycle are more likely to have vulnerabilities that will remain unpatched.

PATCHING CADENCE > ISSUE DETAIL

End-of-Service Product

We observed an end-of-service product, one that is no longer supported by the manufacturer, publicly exposed.

-0.1 SCORE IMPACT

1 finding

PRODUCT MANUFACTURER	PRODUCT NAME	PRODUCT VERSION	STATE EFFECTIVE DATE	STATE REF	LAST SEEN	
Juniper	Netscreen SSL Hardware SA2000	-	2016-03-31	http://www.juniper. net/support/eol/ssl _hw.html		2019-01- 16T05:21:48.000Z

RECOMMENDATION

Replace or upgrade the affected product. Review the vendor's statement of EOS guidelines for replacement products or contact the vendor. In some cases, it may be possible to negotiate a custom support plan for the EOS product.

ABOUT THIS ISSUE

A product that has been declared as end-of-service (EOS) by the manufacturer has been detected. An EOS product is no longer eligible for any support, security patches, or replacement parts. Products at this stage in their life cycle are more likely to have vulnerabilities that need to be patched, but without service support those vulnerabilities will persist until the product is replaced. Using EOS products also violates several compliance frameworks, including PCI DSS and HIPAA.

PATCHING CADENCE > ISSUE DETAIL

Medium Severity CVEs Patching Cadence

Medium severity vulnerability seen on network more than 60 days after CVE was published.

-0.7 SCORE

500 findings

ID	URL	PUBLICATION DATE	DESTINATION IP	DESTINATION PORT	LAST SEEN
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	192.131.72.203	443	2018-12- 16T18:59:11.000Z
(heap-based buffer overf	d_status module in the Apache low), or possibly obtain sensitiv idling within the status_handler ua_request.c.	e credential information or e	xecute arbitrary code, via a c	rafted request that triggers	
CVE-2015-3194	https://nvd.nist.gov/vu In/detail/CVE-2015- 3194	2015-12-06	192.131.72.203	443	2018-12- 16T18:59:11.000Z
	n OpenSSL 1.0.1 before 1.0.1q an application crash) via an RSA P				
CVE-2015-3185	https://nvd.nist.gov/vu	2015-07-20	192.131.72.203	443	2018-12-

	In/detail/CVE-2015-				16T18:59:11.000Z
Description	3185				
directive may be associate	ed function in server/request. d with an authorization setting s in opportunistic circumstand	rather than an authentication	n setting, which allows remote	e attackers to bypass	
CVE-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	192.131.72.203	443	2018-12- 16T18:59:11.000Z
1.0.1m, and 1.0.2 before 1.0.	y function in s2_srvr.c in the S 2a accepts a nonzero CLIENT determine the MASTER-KEY v VE-2016-0800.	-MASTER-KEY CLEAR-KEY-L	ENGTH value for an arbitrary	cipher, which allows man-	
CVE-2015-3197	https://nvd.nist.gov/vu In/detail/CVE-2015- 3197	2016-02-14	192.131.72.203	443	2018-12- 16T18:59:11.000Z
the-middle attackers to def	0.1 before 1.0.1r and 1.0.2 before tryptographic protection I get_client_hello functions.				
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	192.131.72.203	443	2018-12- 16T18:59:11.000Z
lines and headers. Accepting	releases prior to 2.2.32 and 2 ng these different behaviors r plication servers, either throug ng and cache pollution.	epresented a security concer	n when httpd participates in a	any chain of proxies or	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	192.131.72.203	443	2018-12- 16T18:59:11.000Z
remote attackers to conduc	ng implementation in the Apart t HTTP request smuggling at aracters in modules/http/http_	tacks via a crafted request, re			
CVE-2015-3195	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	192.131.72.203	443	2018-12- 16T18:59:11.000Z
1.0.2 before 1.0.2e mishand	E implementation in crypto/as fles errors caused by malform nemory by triggering a decod	ed X509_ATTRIBUTE data, v	vhich allows remote attackers		
CVE-2015-0232	https://nvd.nist.gov/vu In/detail/CVE-2015- 0232	2015-01-27	209.163.213.134	443	2018-12- 16T13:13:28.000Z
	function in ext/exif/exif.c in Pl r cause a denial of service (ui				
CVE-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	209.163.213.134	443	2018-12- 16T13:13:28.000Z
1.0.1m, and 1.0.2 before 1.0.	r function in s2_srvr.c in the S 2a accepts a nonzero CLIENT determine the MASTER-KEY v VE-2016-0800.	-MASTER-KEY CLEAR-KEY-L	ENGTH value for an arbitrary	cipher, which allows man-	

CVE-2014-3597	https://nvd.nist.gov/vu In/detail/CVE-2014- 3597	2014-08-22	209.163.213.134	443	2018-12- 16T13:13:28.000Z
servers to cause a denial	n the php_parserr function in of service (application crash) of and the dn_expand function. N	r possibly execute arbitrary c	ode via a crafted DNS record	, related to the	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	209.163.213.134	443	2018-12- 16T13:13:28.000Z
remote attackers to condu	ing implementation in the Apa uct HTTP request smuggling a naracters in modules/http/http.	ttacks via a crafted request, re			
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	209.163.213.134	443	2018-12- 16T13:13:28.000Z
directive may be associate	red function in server/request ed with an authorization settin ns in opportunistic circumstan	g rather than an authenticatio	n setting, which allows remot	e attackers to bypass	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	209.163.213.134	443	2018-12- 16T13:13:28.000Z
lines and headers. Accept	II releases prior to 2.2.32 and ing these different behaviors opplication servers, either throu ting and cache pollution.	represented a security conce	rn when httpd participates in	any chain of proxies or	
CVE-2015-3197	https://nvd.nist.gov/vu In/detail/CVE-2015- 3197	2016-02-14	209.163.213.134	443	2018-12- 16T13:13:28.000Z
the-middle attackers to de	1.0.1 before 1.0.1r and 1.0.2 before tryptographic protection and get_client_hello functions.	•	·		
CVE-2015-3195	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	209.163.213.134	443	2018-12- 16T13:13:28.000Z
1.0.2 before 1.0.2e mishan	NE implementation in crypto/as Idles errors caused by malforn memory by triggering a decod	ned X509_ATTRIBUTE data, v	which allows remote attackers		
CVE-2014-3670	https://nvd.nist.gov/vu In/detail/CVE-2014- 3670	2014-10-29	209.163.213.134	443	2018-12- 16T13:13:28.000Z
floating-point arrays incor	function in exif.c in the EXIF e. rectly, which allows remote att code via a crafted JPEG imag	ackers to cause a denial of se	ervice (heap memory corruption	on and application crash) or	
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	209.163.213.134	443	2018-12- 16T13:13:28.000Z
	l_status module in the Apache ow), or possibly obtain sensitiv				

				·	
improper scoreboard h function in modules/lua	andling within the status_handle a/lua_request.c.	r function in modules/g	enerators/mod_status.c and the	lua_ap_scoreboard_worker	
CVE-2015-3194	https://nvd.nist.gov/vu In/detail/CVE-2015- 3194	2015-12-06	209.163.213.134	443	2018-12- 16T13:13:28.000Z
	in OpenSSL 1.0.1 before 1.0.1q ar d application crash) via an RSA P				
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	192.131.76.100	443	2018-12- 15T14:29:43.000Z
	quired function in server/request				

intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 192.131.76.100 2018-12-443 In/detail/CVE-2017-15T14:29:43.000Z

3737

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2015-3183 2015-07-20 192.131.76.100 443 2018-12https://nvd.nist.gov/vu In/detail/CVE-2015-15T14:29:43.000Z 3183

Description:

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 192.131.76.100 443 2018-12-In/detail/CVE-2017-15T14:29:43.000Z

3738

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 192.131.76.100 443 2018-12-

In/detail/CVE-2014-

0226

15T14:29:43.000Z

Description:

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 192.131.76.100 443 2018-12-In/detail/CVE-2017-15T14:29:43.000Z

3736

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

processors that support th	e BMI1, BMI2 and ADX extens	sions like Intel Broadwell (5th	generation) and later or AMD	Ryzen.	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	192.131.76.100	443	2018-12- 15T14:29:43.000Z
lines and headers. Accept	I releases prior to 2.2.32 and ing these different behaviors plication servers, either throu ing and cache pollution.	represented a security conce	rn when httpd participates in	any chain of proxies or	
CVE-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	209.163.213.134	80	2018-12- 11T04:15:36.000Z
1.0.1m, and 1.0.2 before 1.0	y function in s2_srvr.c in the \$.2a accepts a nonzero CLIEN determine the MASTER-KEY \ VE-2016-0800.	T-MASTER-KEY CLEAR-KEY-I	ENGTH value for an arbitrary	cipher, which allows man-	
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	209.163.213.134	80	2018-12- 11T04:15:36.000Z
(heap-based buffer overflo	_status module in the Apache w), or possibly obtain sensitiv dling within the status_handle a_request.c.	e credential information or ex	xecute arbitrary code, via a cr	afted request that triggers	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	209.163.213.134	80	2018-12- 11T04:15:36.000Z
lines and headers. Accept	I releases prior to 2.2.32 and ing these different behaviors oplication servers, either through and cache pollution.	represented a security conce	rn when httpd participates in	any chain of proxies or	
CVE-2015-3195	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	209.163.213.134	80	2018-12- 11T04:15:36.000Z
1.0.2 before 1.0.2e mishan	IE implementation in crypto/as dles errors caused by malforn nemory by triggering a decod	ned X509_ATTRIBUTE data,	which allows remote attacker	.0t, 1.0.1 before 1.0.1q, and s to obtain sensitive	
CVE-2015-0232	https://nvd.nist.gov/vu In/detail/CVE-2015- 0232	2015-01-27	209.163.213.134	80	2018-12- 11T04:15:36.000Z
	e function in ext/exif/exif.c in P or cause a denial of service (u	,	'		
CVE-2015-3197	https://nvd.nist.gov/vu In/detail/CVE-2015- 3197	2016-02-14	209.163.213.134	80	2018-12- 11T04:15:36.000Z

Description

ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.

CVE-2014-3670	https://nvd.nist.gov/vu In/detail/CVE-2014- 3670	2014-10-29	209.163.213.134	80	2018-12- 11T04:15:36.000Z
floating-point arrays inco	e function in exif.c in the EXIF ex prectly, which allows remote att ry code via a crafted JPEG imag	ackers to cause a denial of se	ervice (heap memory corrupti	on and application crash) or	
CVE-2015-3194	https://nvd.nist.gov/vu In/detail/CVE-2015- 3194	2015-12-06	209.163.213.134	80	2018-12- 11T04:15:36.000Z
	n OpenSSL 1.0.1 before 1.0.1q ar application crash) via an RSA P				
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	209.163.213.134	80	2018-12- 11T04:15:36.000Z
directive may be associa	uired function in server/request. Ited with an authorization setting ons in opportunistic circumstan	g rather than an authenticatio	n setting, which allows remot	e attackers to bypass	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	209.163.213.134	80	2018-12- 11T04:15:36.000Z
remote attackers to cond	ding implementation in the Apa duct HTTP request smuggling at characters in modules/http/http.	ttacks via a crafted request, r			
CVE-2014-3597	https://nvd.nist.gov/vu In/detail/CVE-2014- 3597	2014-08-22	209.163.213.134	80	2018-12- 11T04:15:36.000Z
servers to cause a denia	s in the php_parserr function in o I of service (application crash) o a and the dn_expand function. N	r possibly execute arbitrary c	ode via a crafted DNS record	, related to the	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	64.149.172.164	443	2018-12- 07T20:20:28.426Z
	used in OpenSSL through 1.0.1i kers to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	209.222.72.13	443	2018-12- 07T11:12:33.427Z
	used in OpenSSL through 1.0.1i kers to obtain cleartext data via			which makes it easier for	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	166.73.92.20	443	2018-12- 01T09:53:55.225Z
lines and headers. Acceptinteracts with back-end a	all releases prior to 2.2.32 and pting these different behaviors rapplication servers, either throughting and cache pollution.	represented a security conce	rn when httpd participates in	any chain of proxies or	

CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	166.73.92.20	443	2018-12- 01T09:53:55.225Z
directive may be associated	ed function in server/request. d with an authorization setting s in opportunistic circumstand	g rather than an authenticatio	n setting, which allows remot	e attackers to bypass	
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	166.73.92.20	443	2018-12- 01T09:53:55.225Z
(heap-based buffer overflow	_status module in the Apache w), or possibly obtain sensitiv ling within the status_handler _request.c.	e credential information or ex	ecute arbitrary code, via a cra	afted request that triggers	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	166.73.92.20	443	2018-12- 01T09:53:55.225Z
remote attackers to conduc	ng implementation in the Apa ct HTTP request smuggling at aracters in modules/http/http_	ttacks via a crafted request, re			
CVE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	166.73.92.20	443	2018-12- 01T09:53:55.225Z
handshake then OpenSSL as designed for the explicit work correctly if SSL_read(initial function call. If SSL_re is passed without being dehave to be present that res	m version 1.0.2b) introduced a would move into the error static handshake functions (SSL_d) or SSL_write() is called directed()/SSL_write() is subseque crypted/encrypted directly froulted in a call to SSL_read()/SFixed in OpenSSL 1.0.2n. Open	ate and would immediately fai o_handshake(), SSL_accept() ttly. In that scenario, if the har intly called by the application om the SSL/TLS record layer. SSL_write() being issued after	I if you attempted to continue and SSL_connect()), howevendshake fails then a fatal error for the same SSL object then In order to exploit this issue a	the handshake. This works r due to a bug it does not r will be returned in the it will succeed and the data an application bug would	
CVE-2017-3738	https://nvd.nist.gov/vu In/detail/CVE-2017- 3738	2017-12-07	166.73.92.20	443	2018-12- 01T09:53:55.225Z
are affected. Analysis sugg believed likely. Attacks aga private key may be perform TLS to be meaningful, the s 2016-0701. This only affects from this issue is similar to Fixed in OpenSSL 1.0.2n. D	in the AVX2 Montgomery multi- lests that attacks against RSA sinst DH1024 are considered j ned offline. The amount of res- server would have to share the server would have to share the server would have to share the cVE-2017-3736, CVE-2017-37 true to the low severity of this when it becomes available. The	and DSA as a result of this d just feasible, because most o sources required for such an a e DH1024 private key among AVX2 but not ADX extension 32 and CVE-2015-3193. Ope issue we are not issuing a ne	efect would be very difficult to f the work necessary to dedu attack would be significant. H i multiple clients, which is no I as like Intel Haswell (4th gene inSSL version 1.0.2-1.0.2m and w release of OpenSSL 1.1.0 at	o perform and are not ce information about a owever, for an attack on onger an option since CVE- rration). Note: The impact 11.0-1.1.0g are affected. this time. The fix will be	
CVE-2017-3736	https://nvd.nist.gov/vu In/detail/CVE-2017- 3736	2017-11-02	166.73.92.20	443	2018-12- 01T09:53:55.225Z
algorithms are affected. An are not believed likely. Atta information about a private likely only accessible to a li target private key in a scen	g bug in the x86_64 Montgon alysis suggests that attacks a acks against DH are considers key may be performed offlin- imited number of attackers. A lario with persistent DH paran e BMI1, BMI2 and ADX extens	gainst RSA and DSA as a res ed just feasible (although very e. The amount of resources r n attacker would additionally neters and a private key that	ult of this defect would be ver difficult) because most of the equired for such an attack wo need online access to an ung is shared between multiple cl	ry difficult to perform and e work necessary to deduce ould be very significant and patched system using the ients. This only affects	
CVE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	208.11.141.76	443	2018-12- 01T05:12:05.184Z

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.11.141.76 443 2018-12-

In/detail/CVE-2017-01T05:12:05.184Z

3736

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.76 443 2018-12-

In/detail/CVE-2016-

8743

01T05:12:05.184Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.11.141.76 443 2018-12-

In/detail/CVE-2017-01T05:12:05.184Z 3738

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.11.141.76 443 2018-12-In/detail/CVE-2015-

3183

01T05:12:05.184Z

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208 11 141 76 443 2018-12-

In/detail/CVE-2014-

01T05:12:05.184Z

0226

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.76 443 2018-12-

In/detail/CVE-2015-

3185

01T05:12:05.184Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require

directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

2017-12-07 208.11.141.132 CVE-2017-3738 https://nvd.nist.gov/vu 443 2018-11-

30T19:25:11.325Z In/detail/CVE-2017-

3738

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository

CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 208.11.141.132 443 2018-11-

In/detail/CVE-2017-

3737

30T19:25:11.325Z

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

https://nvd.nist.gov/vu CVE-2015-3185 2015-07-20 208.11.141.132 443 2018-11-

In/detail/CVE-2015-

3185

30T19:25:11.325Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.132 443 2018-11-

In/detail/CVE-2014-

0226

30T19:25:11.325Z

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.11.141.132 443 2018-11-

In/detail/CVE-2017-

3736

30T19:25:11.325Z

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2016-8743 2017-07-27 208.11.141.132 https://nvd.nist.gov/vu 443 2018-11-30T19:25:11.325Z

In/detail/CVE-2016-

8743

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	208.11.141.132	443	2018-11- 30T19:25:11.325Z		
Description:							
The chunked transfer cod remote attackers to condu	ling implementation in the Apa uct HTTP request smuggling at haracters in modules/http/http_	ttacks via a crafted request, re					
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	208.11.141.88	443	2018-11- 30T18:54:11.321Z		
directive may be associate	ired function in server/request. ed with an authorization setting ins in opportunistic circumstance	g rather than an authenticatio	n setting, which allows remote	e attackers to bypass			
CVE-2017-3736	https://nvd.nist.gov/vu In/detail/CVE-2017- 3736	2017-11-02	208.11.141.88	443	2018-11- 30T18:54:11.321Z		
Description:							
There is a carry propagati algorithms are affected. A are not believed likely. At information about a privat likely only accessible to a target private key in a sce	ng bug in the x86_64 Montgor nalysis suggests that attacks a tacks against DH are considere e key may be performed offlin- limited number of attackers. A enario with persistent DH paran ne BMI1, BMI2 and ADX extens	gainst RSA and DSA as a res ed just feasible (although very e. The amount of resources r in attacker would additionally neters and a private key that	ult of this defect would be ver difficult) because most of the equired for such an attack wo need online access to an unp is shared between multiple cli	y difficult to perform and work necessary to deduce uld be very significant and vatched system using the ents. This only affects			
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	208.11.141.88	443	2018-11- 30T18:54:11.321Z		
lines and headers. Accept	Ill releases prior to 2.2.32 and it ting these different behaviors re oplication servers, either through ting and cache pollution.	represented a security conce	rn when httpd participates in a	ny chain of proxies or			
CVE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	208.11.141.88	443	2018-11- 30T18:54:11.321Z		
handshake then OpenSSI as designed for the explic work correctly if SSL_reac initial function call. If SSL_is passed without being dhave to be present that re	Description: DeenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a andshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works is designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data a passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would a ave to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.						
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	208.11.141.88	443	2018-11- 30T18:54:11.321Z		
(heap-based buffer overflo	d_status module in the Apache ow), or possibly obtain sensitiv dling within the status_handler a_request.c.	e credential information or ex	ecute arbitrary code, via a cra	fted request that triggers			
CVE-2017-3738	https://nvd.nist.gov/vu In/detail/CVE-2017- 3738	2017-12-07	208.11.141.88	443	2018-11- 30T18:54:11.321Z		
are affected. Analysis sug	in the AVX2 Montgomery mult gests that attacks against RSA gainst DH1024 are considered	and DSA as a result of this d	efect would be very difficult to	perform and are not			

17T18:30:12.000Z

private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact for this issue is similar to CVE-2017-3732, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n, Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.11.141.88 443 2018-11-

In/detail/CVE-2015- 30T18:54:11.321Z

3183

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2015-3194 https://nvd.nist.gov/vu 2015-12-06 208.11.141.155 443 2018-11-

In/detail/CVE-2015- 17T18:30:12.000Z

3194

Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.

.....

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.155 443 2018-11-

8743

In/detail/CVE-2016-

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request

smuggling, response splitting and cache pollution.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.155 443 2018-11-

In/detail/CVE-2015- 17T18:30:12.000Z

3185

Description:
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2016-0703 https://nvd.nist.gov/vu 2016-03-02 208.11.141.155 443 2018-11-

In/detail/CVE-2016- 17T18:30:12.000Z

0703

Description:
The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows manin-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding

ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-

CVE-2015-3197 https://nvd.nist.gov/vu 2016-02-14 208.11.141.155 443 2018-11-

In/detail/CVE-2015- 17T18:30:12.000Z 3197

Description:

Description:

oracle, a related issue to CVE-2016-0800.

the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.155 443 2018-11-

In/detail/CVE-2014- 17T18:30:12.000Z

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	208.11.141.155	443	2018-11- 17T18:30:12.000Z	
remote attackers to cond	ding implementation in the Apa duct HTTP request smuggling at characters in modules/http/http_	tacks via a crafted request, r				
CVE-2015-3195	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	208.11.141.155	443	2018-11- 17T18:30:12.000Z	
1.0.2 before 1.0.2e misha	INE implementation in crypto/as andles errors caused by malform s memory by triggering a decod	ed X509_ATTRIBUTE data,	which allows remote attackers			
CVE-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	63.240.88.6	443	2018-11- 16T08:28:28.000Z	
1.0.1m, and 1.0.2 before 1	key function in s2_srvr.c in the S .0.2a accepts a nonzero CLIENT o determine the MASTER-KEY v CVE-2016-0800.	Γ-MASTER-KEY CLEAR-KEY-I	ENGTH value for an arbitrary	cipher, which allows man-		
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	63.240.88.6	443	2018-11- 16T08:28:28.000Z	
lines and headers. Acceptinteracts with back-end a	all releases prior to 2.2.32 and 2 oting these different behaviors r application servers, either through itting and cache pollution.	epresented a security conce	rn when httpd participates in a	any chain of proxies or		
CVE-2015-3197	https://nvd.nist.gov/vu In/detail/CVE-2015- 3197	2016-02-14	64.128.99.203	443	2018-11- 15T14:09:57.000Z	
the-middle attackers to o	. 1.0.1 before 1.0.1r and 1.0.2 before the cryptographic protection and get_client_hello functions.					
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	64.128.99.203	443	2018-11- 15T14:09:57.000Z	
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.						
CVE-2015-3195	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	64.128.99.203	443	2018-11- 15T14:09:57.000Z	
1.0.2 before 1.0.2e misha	INE implementation in crypto/as andles errors caused by malform a memory by triggering a decod	ed X509_ATTRIBUTE data,	which allows remote attackers			
CVE-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	64.128.99.203	443	2018-11- 15T14:09:57.000Z	
Description:			nSSL before 0.9.8zf, 1.0.0 bef			

VE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	64.128.99.203	443	2018-11- 15T14:09:57.000Z	
nes and headers. Acce teracts with back-end	all releases prior to 2.2.32 and a pting these different behaviors of application servers, either through litting and cache pollution.	represented a security c	oncern when httpd participates	in any chain of proxies	or	
VE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	64.128.99.203	443	2018-11- 15T14:09:57.000Z	
mote attackers to con	oding implementation in the Apa duct HTTP request smuggling at characters in modules/http/http_	ttacks via a crafted requ				
VE-2015-3194	https://nvd.nist.gov/vu In/detail/CVE-2015- 3194	2015-12-06	64.128.99.203	443	2018-11- 15T14:09:57.000Z	
_	in OpenSSL 1.0.1 before 1.0.1q an d application crash) via an RSA P			,	L	
VE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	64.128.99.203	443	2018-11- 15T14:09:57.000Z	
irective may be associa	quired function in server/request. ated with an authorization setting ions in opportunistic circumstance	g rather than an authent	ication setting, which allows re	mote attackers to bypas	s	
VE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	63.251.77.220	443	2018-11- 09T13:22:52.450Z	
	s used in OpenSSL through 1.0.1i kers to obtain cleartext data via			ng, which makes it easie	r for	
:VE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	12.16.165.109	443	2018-11- 08T08:40:47.752Z	
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.						
VE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	64.128.99.68	443	2018-11- 06T23:51:02.464Z	
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.						
VE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	64.128.99.60	443	2018-11- 06T23:50:23.700Z	
escription:						

CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	64.128.99.65	443	2018-11- 06T23:32:23.425Z		
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for			
CVE-2017-5647	https://nvd.nist.gov/vu In/detail/CVE-2017- 5647	2017-04-17	198.167.0.33	443	2018-10- 23T01:30:22.924Z		
and 6.0.0 to 6.0.52, wher completed. This could res	the pipelined requests in Apacl n send file was used, results in sult in responses appearing to esponse for request A, the resp	the pipelined request being be sent for the wrong reques	ost when send file processing t. For example, a user agent t	g of the previous request hat sent requests A, B and			
CVE-2015-3194	https://nvd.nist.gov/vu In/detail/CVE-2015- 3194	2015-12-06	192.131.76.100	443	2018-10- 22T11:12:21.001Z		
	ı OpenSSL 1.0.1 before 1.0.1q ar application crash) via an RSA P						
CVE-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	192.131.76.100	443	2018-10- 22T11:12:21.001Z		
1.0.1m, and 1.0.2 before 1.	ey function in s2_srvr.c in the 9 0.2a accepts a nonzero CLIEN o determine the MASTER-KEY v CVE-2016-0800.	T-MASTER-KEY CLEAR-KEY-I	ENGTH value for an arbitrary	cipher, which allows man-			
CVE-2015-3197	https://nvd.nist.gov/vu In/detail/CVE-2015- 3197	2016-02-14	192.131.76.100	443	2018-10- 22T11:12:21.001Z		
the-middle attackers to de	1.0.1 before 1.0.1r and 1.0.2 bef efeat cryptographic protection nd get_client_hello functions.						
CVE-2015-3195	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	192.131.76.100	443	2018-10- 22T11:12:21.001Z		
1.0.2 before 1.0.2e mishar	Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.						
CVE-2016-0800	https://nvd.nist.gov/vu In/detail/CVE-2016- 0800	2016-03-01	50.58.10.133	443	2018-10- 22T09:47:25.478Z		
message before establish	sed in OpenSSL before 1.0.1s a ning that a client possesses ce ging a Bleichenbacher RSA pa	rtain plaintext RSA data, whic	h makes it easier for remote a				
CVE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	166.73.6.220	443	2018-10- 21T18:56:59.069Z		
	om version 1.0.2b) introduced L would move into the error sta						

as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 166.73.6.220 443 2018-10-In/detail/CVE-2017-21T18:56:59.069Z

3736

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 166.73.6.220 443 2018-10-In/detail/CVE-2016-21T18:56:59.069Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2014-0226 2014-07-20 https://nvd.nist.gov/vu 166.73.6.220 443 2018-10-

In/detail/CVE-2014-

0226

21T18:56:59.069Z

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 166.73.6.220 443 2018-10-

In/detail/CVE-2017-

3738

21T18:56:59.069Z

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 166.73.6.220 443 2018-10-

In/detail/CVE-2015-

3185

21T18:56:59.069Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2015-3183 https://nvd.nist.gov/vu 2018-10-2015-07-20 166.73.6.220 443

In/detail/CVE-2015-

3183

21T18:56:59.069Z

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2014-3566 https://mcl.nist.gov/us 2014-10-14 12.14.174.232 636 2018-10-11TB83107.0002 15166								
The SSL protocol 3.0, as used in OpenSSL through 1.0 til and other products, uses nondeterministic CBC padding, which makes it easier for manner that middle intellies but beliance intellies of the protocol of the products of the protocol	CVE-2014-3566	In/detail/CVE-2014-	2014-10-14	12.14.174.232	636			
InvidenticVE-2014-3566 Description The SSL protocol 3.0 as used in OpenSSL through 1.0 til and other products, uses nondeterministic CBC padding, which makes it easier for mann-in-theriteridide attackers to obtain clearhext data via a padding-oracle attack, aka the "POODLE" issue. CVE-2014-3566 https://ruvd.nist.gov/vu 2014-10-14	The SSL protocol 3.0, as u				which makes it easier for			
The SSL protocol 3.0, as used in OpenSSL through 1.0.1 and other products, uses nondeterministic C8C padding, which makes it easier for man in the middle tableckers to bottimic incentrate data via a padding-protocol tableck, set the "POOLE" Issue. CVE-2014-3566 https://mvd.nist.gov/vu 2014-10-14 50.58.9.48 443 2018-10-3716-3566 Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.8 and other products, uses nondeterministic C8C padding, which makes it easier for man in-the-middle attackers to obtain clearated data via a padding-protocle attack, aka the "POODLE" issue. CVE-2014-3566 https://mvd.nist.gov/vu 2014-10-14 50.58.9.181 443 2018-10-970117.35.0002 Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.18 and other products, uses nondeterministic C8C padding, which makes it easier for man in-the-middle attackers to obtain clearated totat via a padding-protocle attack, aka the "POODLE" issue. CVE-2016-0800 https://mvd.nist.gov/vu 2016-03-01 209.163.213.137 443 2018-10-9000 2011/17.35.0002 Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.18 and other products, uses nondeterministic C8C padding, which makes it easier for man-in-the-middle attackers to obtain clearated totat via a padding-protocle attack, aka the "POODLE" issue. CVE-2016-0800 https://mvd.nist.gov/vu 2016-03-01 209.163.213.137 443 2018-00 0711042.39.0002 Description: The SSL2p protocol, as used in OpenSSL before 1.0.1s and 0.1.0.2 before 1.0.2g and other products, requires a server to send a ServetVerilly message before establishing that a client possesses certain plaintext RSA padding ornote, aka a "DROWN" attack. CVE-2017-3737 https://mvd.nist.gov/vu 2017-12-07 208.66.20.31 443 2018-09-15115-20.24.8092 Description: Description: CyperSSL veral more in the error state and wastal immediately fail if you attempted to continue the handstake. This works as designed for the explicit handshake functions (SSL , dc.) bendshake, SSL , accept) and SSL , connectly, however due to a bug if does not work c	CVE-2014-3566	In/detail/CVE-2014-	2014-10-14	64.149.172.103	443			
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1 and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle intackers to obtain clearance data via a padding-oracle attack, also the "POODLE" issue. CVE-2014-3566	The SSL protocol 3.0, as u				which makes it easier for			
The SSL protocol 3.0, as used in OpenSSL through 1.0.1 and other products, uses nondeterministic CBC padding, which makes it easier for manner the medical etackers to other objects and a second of the products of the produ	CVE-2014-3566	In/detail/CVE-2014-	2014-10-14	50.58.9.48	443			
In/detail/CVE-2014- 3566 Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1 and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attrackers to obtain cleariest data via a padding-oracle attrack, also the "POOLE" issue. CVE-2016-0800 https://mvd.nist.gov/vu 2016-03-01 209.163.213.137 443 2018-10- 07710-42:39.0002 Description: The SSLV2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintex RSA data, which makes it easier for remote attrackers to decrypt TLS ophertext data by leveraging a Biolehenbacker RSA padding oracle, also a "DROWN" attack. CVE-2017-3737 https://mvd.nist.gov/vu 2017-12-07 208.66.20.31 443 2018-09- 15715;20:24.8092 Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake functions (SSL, do_p.nandshake(), SSL_acceptl) and SSL_connect()), however due to a bug it does not work correctly it SSL_redol or SSL_write() is called directly. In that scenario, if the handshake falls then a final error via trutued in the initial function call. if SSL_redol(SSL_write) is aubsequently called by the application for the same SSL object them via succeed and rule data was to be present that resulted in a roal the SSL_redol(SSL_write) is aubsequently called by the application for the same SSL object them via succeed and rule data was to be present that resulted in a roal the SSL_redol(SSL_write) is aubsequently called by the application for the same SSL object them via succeed and rule data was to be present that resulted in a roal the SSL_redol(SSL_write) being issued after having already received a fatal error via trutued in the initial function call. if SSL_redol(SSL_write) is aubsequently called by the application for the same SSL object them via succeed and rule data was to be present that resulted	The SSL protocol 3.0, as u				which makes it easier for			
The SSL protocol 3.0, as used in OpenSSL through 1.0.1 in and other products, uses nondeterministic CBC padding, which makes it easier for mann-in-the-middle attackers to obtain clearted taids via a padding-oracle attack, also the "POODLE" issue. CVE-2016-0800 https://nvd.nist.gov/vu 2016-03-01 209.163.213.137 443 2018-10-07T10:42:39.0002 0800 Description: The SSLv2 protocol, as used in OpenSSL before 10.1s and 10.2 before 10.2g and other products, requires a server to send a Server/Verify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack. CVE-2017-3737 https://nvd.nist.gov/vu ln/detail/CVE-2017-37377 Description: OpenSSL 10.2 (starting from version 10.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fall if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL do. handshake), SSL accipacity and SSL_comberQil) and SSL_comberQil an	CVE-2014-3566	In/detail/CVE-2014-	2014-10-14	50.58.9.181	443			
Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a cilient possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack. CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 208.66.20.31 443 2018-09-15T15-20:24.809Z 15T15-20:24.809Z 15T15-20:24	The SSL protocol 3.0, as u				which makes it easier for			
The SSLv2 protocol, as used in OpenSSL before 1.01s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client prossesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack. CVE-2017-3737 https://nvd.nist.gov/vu ln/detail/CVE-2017-3737 ln/detail/CVE-2017-3737 https://nvd.nist.gov/vu ln/detail/CVE-2017-3737 ln/detail/CVE-2017-3737 ln/detail/CVE-2017-3737 ln/detail/CVE-2017-3737 ln/detail/CVE-2017-3737 ln/detail/CVE-2017-3737 ln/detail/CVE-2017-3737 ln/detail/CVE-2017-3737 ln/detail/CVE-2017-3738 ln/detail/	CVE-2016-0800	In/detail/CVE-2016-	2016-03-01	209.163.213.137	443			
In/detail/CVE-2017-3737 Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fall if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake falls then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected. CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.66.20.31 443 2018-09-15T15:20:24.809Z 3738 Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against BSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH024 private key among multiple clinding mild the flam on the private key among multiple clinding mild the generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. Ope	The SSLv2 protocol, as us message before establishing	ing that a client possesses cer	tain plaintext RSA data, which	h makes it easier for remote a				
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(i), SSL_accept) and SSL_connect(j), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. if SSL_read() SSL_write() is subsequently called by the application for besame SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.10 is not affected. CVE-2017-3738	CVE-2017-3737	In/detail/CVE-2017-	2017-12-07	208.66.20.31	443			
In/detail/CVE-2017-3738 Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0 h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository. CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.66.20.31 443 2018-09-	OpenSSL 1.0.2 (starting fro handshake then OpenSSL as designed for the explici work correctly if SSL_read initial function call. If SSL_i is passed without being do have to be present that re-	OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLs record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version						
There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository. CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.66.20.31 443 2018-09-	CVE-2017-3738	In/detail/CVE-2017-	2017-12-07	208.66.20.31	443			
·	There is an overflow bug i are affected. Analysis suggesteleved likely. Attacks ag private key may be perfort TLS to be meaningful, the 2016-0701. This only affect from this issue is similar to Fixed in OpenSSL 1.0.2n. I	gests that attacks against RSA ainst DH1024 are considered j med offline. The amount of res server would have to share th ts processors that support the CVE-2017-3736, CVE-2017-37 Due to the low severity of this	and DSA as a result of this d just feasible, because most o sources required for such an e DH1024 private key among AVX2 but not ADX extension 732 and CVE-2015-3193. Ope issue we are not issuing a ne	efect would be very difficult to f the work necessary to dedu attack would be significant. H g multiple clients, which is no I ns like Intel Haswell (4th gene nSSL version 1.0.2-1.0.2m and w release of OpenSSL 1.1.0 at	o perform and are not ce information about a owever, for an attack on onger an option since CVE- rration). Note: The impact 11.0-1.1.0g are affected. this time. The fix will be			
	CVE-2017-3736		2017-11-02	208.66.20.31	443			

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2014-3566

https://nvd.nist.gov/vu In/detail/CVE-20142014-10-14

64.149.172.167

443

2018-09-10T15:45:49.000Z

3566

Description:

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2014-3566

https://nvd.nist.gov/vu In/detail/CVE-2014-

3566

2014-10-14

204.95.150.235

2018-09-

08T23:06:23.000Z

Description:

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2014-3566

https://nvd.nist.gov/vu In/detail/CVE-20142014-10-14

204.95.150.237

2018-09-

08T22:58:36.000Z

3566

Description:

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVF-2014-3566

https://nvd.nist.gov/vu In/detail/CVE-2014-

2014-10-14

166 73 11 22

2018-09-

07T12:28:01.000Z

3566

3566

5647

3736

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue

CVE-2014-3566

https://nvd.nist.gov/vu In/detail/CVE-20142014-10-14

204.95.150.213

2018-09-

07T10:50:12.000Z

Description:

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2017-5647

https://nvd.nist.gov/vu In/detail/CVE-20172017-04-17

198.167.0.148

2018-08-

18T07:58:01.000Z

Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.

CVE-2017-3736

https://nvd.nist.gov/vu In/detail/CVE-20172017-11-02

192.131.76.23

443

2018-08-

17T09:55:55.000Z

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects

ocessors that support	t the BMI1, BMI2 and ADX extens	ions like Intel Broadwe	ell (5th generation) and later or	AMD Ryzen.	
VE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	192.131.76.23	443	2018-08- 17T09:55:55.000Z
andshake then OpenS designed for the exp ork correctly if SSL_re itial function call. If SS passed without being ave to be present that	from version 1.0.2b) introduced a SSL would move into the error stabilicit handshake functions (SSL_dead() or SSL_write() is called direct_read()/SSL_write() is subsequeg decrypted/encrypted directly from the stability of the s	ate and would immedia o_handshake(), SSL_a titly. In that scenario, if the ntly called by the application the SSL/TLS record title.	tely fail if you attempted to cor ccept() and SSL_connect()), how he handshake fails then a fatal cation for the same SSL object layer. In order to exploit this is d after having already received	tinue the handshake. This wever due to a bug it does error will be returned in th then it will succeed and th sue an application bug wo	not ee ee data uld
VE-2017-3738	https://nvd.nist.gov/vu In/detail/CVE-2017- 3738	2017-12-07	192.131.76.23	443	2018-08- 17T09:55:55.000Z
e affected. Analysis si elieved likely. Attacks ivate key may be perf LS to be meaningful, ti 016-0701. This only aff om this issue is similar xed in OpenSSL 1.0.2	ig in the AVX2 Montgomery mult uggests that attacks against RSA against DH1024 are considered formed offline. The amount of res he server would have to share th fects processors that support the r to CVE-2017-3736, CVE-2017-37 n. Due to the low severity of this 1.0h when it becomes available.	and DSA as a result of just feasible, because i sources required for su e DH1024 private key a AVX2 but not ADX ex 232 and CVE-2015-3193 issue we are not issuin	f this defect would be very diffi most of the work necessary to ch an attack would be significa among multiple clients, which i tensions like Intel Haswell (4th 3. OpenSSL version 1.0.2-1.0.2 g a new release of OpenSSL 1.	cult to perform and are not deduce information about ant. However, for an attack s no longer an option since generation). Note: The impn and 1.1.0-1.1.0g are affect 1.0 at this time. The fix will	: a on o CVE- oact ed.
VE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	192.131.76.23	443	2018-08- 17T09:55:55.000Z
rective may be associ	quired function in server/request. iated with an authorization setting tions in opportunistic circumstan	g rather than an auther	ntication setting, which allows r	emote attackers to bypass	
VE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	192.131.76.23	443	2018-08- 17T09:55:55.000Z
eap-based buffer ove	nod_status module in the Apache rflow), or possibly obtain sensitiv andling within the status_handler /lua_request.c.	e credential informatio	n or execute arbitrary code, via	a crafted request that trig	gers
VE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	192.131.76.23	443	2018-08- 17T09:55:55.000Z
es and headers. Acce teracts with back-end	n all releases prior to 2.2.32 and epting these different behaviors rapplication servers, either throughlitting and cache pollution.	epresented a security	concern when httpd participate	es in any chain of proxies o	r
VE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	192.131.76.23	443	2018-08- 17T09:55:55.000Z

198.167.0.246

2018-08-

16T20:57:24.000Z

CVE-2017-5647

https://nvd.nist.gov/vu

In/detail/CVE-2017-

5647

2017-04-17

Desc	

A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.

CVE-2017-5647 https://nvd.nist.gov/vu 2017-04-17 198.167.0.48 2018-08-

In/detail/CVE-2017-16T19:27:59.000Z

5647

A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.

CVE-2015-3195 https://nvd.nist.gov/vu 2015-12-06 208.235.248.231 443 2018-08-

> In/detail/CVE-2015-16T14:03:13.000Z

3195

Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive

CVE-2015-3185 https://nvd.nist.gov/vu 2018-08-2015-07-20 208.235.248.231

In/detail/CVE-2015-

information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.

3185

16T14:03:13.000Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.235.248.231 443 2018-08-

In/detail/CVE-2014-

0226

16T14:03:13.000Z

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3197 https://nvd.nist.gov/vu 2016-02-14 208.235.248.231 443 2018-08-

In/detail/CVE-2015-

3197

16T14:03:13.000Z

ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-inthe-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.

CVE-2015-3194 2015-12-06 2018-08https://nvd.nist.gov/vu 208.235.248.231 443

In/detail/CVE-2015-

3194

16T14:03:13.000Z

Description:

cryptorsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.

CVE-2015-3183 2018-08https://nvd.nist.gov/vu 2015-07-20 443

In/detail/CVE-2015-

3183

208.235.248.231

16T14:03:13.000Z

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2016-0703 https://nvd.nist.gov/vu 2016-03-02 208.235.248.231 443 2018-08-

> In/detail/CVE-2016-16T14:03:13.000Z

	0703				
1.0.1m, and 1.0.2 before 1.0	y function in s2_srvr.c in the S .2a accepts a nonzero CLIEN determine the MASTER-KEY v CVE-2016-0800.	T-MASTÉR-KEY CLEAR-KEY-L	ENGTH value for an arbitrary	cipher, which allows man-	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	208.235.248.231	-	2018-08- 16T14:03:13.000Z
lines and headers. Accepti	I releases prior to 2.2.32 and ing these different behaviors in plication servers, either throughing and cache pollution.	epresented a security concer	rn when httpd participates in a	any chain of proxies or	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	64.149.172.137	443	2018-08- 16T04:41:32.000Z
lines and headers. Accepti	I releases prior to 2.2.32 and ing these different behaviors in plication servers, either throughing and cache pollution.	represented a security concer	rn when httpd participates in a	any chain of proxies or	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	64.128.99.71	443	2018-08- 12T15:14:23.000Z
	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via			which makes it easier for	
CVE-2015-0204	https://nvd.nist.gov/vu In/detail/CVE-2015- 0204	2015-01-08	209.163.213.118	-	2018-08- 12T14:31:57.000Z
	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via			which makes it easier for	
CVE-2016-0800	https://nvd.nist.gov/vu In/detail/CVE-2016- 0800	2016-03-01	209.163.213.118	-	2018-08- 12T14:31:57.000Z
message before establishi	ed in OpenSSL before 1.0.1s a ng that a client possesses cer ing a Bleichenbacher RSA pao	tain plaintext RSA data, which	n makes it easier for remote a		
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	209.163.213.118	443	2018-08- 12T14:31:57.000Z
	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	208.235.248.43	443	2018-08- 11T13:02:46.000Z
	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via			which makes it easier for	
CVE-2017-5647	https://nvd.nist.gov/vu In/detail/CVE-2017-	2017-04-17	198.167.0.133	-	2018-08- 11T13:00:12.558Z

	5647				
and 6.0.0 to 6.0.52, when completed. This could resu	ne pipelined requests in Apach send file was used, results in ult in responses appearing to sponse for request A, the resp	the pipelined request being lobe sent for the wrong request	ost when send file processing t. For example, a user agent t	of the previous request hat sent requests A, B and	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	198.167.0.248	-	2018-08- 11T11:06:11.000Z
lines and headers. Accept	I releases prior to 2.2.32 and ing these different behaviors replication servers, either throughing and cache pollution.	represented a security concer	n when httpd participates in a	any chain of proxies or	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	208.74.12.10	443	2018-08- 11T08:57:55.511Z
lines and headers. Accept	I releases prior to 2.2.32 and ing these different behaviors in plication servers, either throughing and cache pollution.	represented a security concer	n when httpd participates in a	any chain of proxies or	
CVE-2016-0800	https://nvd.nist.gov/vu In/detail/CVE-2016- 0800	2016-03-01	64.149.172.137	-	2018-08- 11T03:56:15.536Z
message before establishi	ed in OpenSSL before 1.0.1s a ing that a client possesses cer ing a Bleichenbacher RSA pao	tain plaintext RSA data, which	n makes it easier for remote a		
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	67.63.175.70	-	2018-08- 11T03:10:42.000Z
	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	208.11.141.38	443	2018-08- 10T20:27:35.000Z
	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via			which makes it easier for	
CVE-2016-0800	https://nvd.nist.gov/vu In/detail/CVE-2016- 0800	2016-03-01	205.219.236.229	443	2018-08- 10T06:51:35.000Z
message before establishi	ed in OpenSSL before 1.0.1s a ing that a client possesses cer ing a Bleichenbacher RSA pao	tain plaintext RSA data, which	n makes it easier for remote a		
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	208.235.248.86	-	2018-08- 10T02:38:55.000Z
•	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via	·		which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu	2014-10-14	208.235.248.122	443	2018-08-

	In/detail/CVE-2014-				10T02:33:12.000Z
	3566				
	sed in OpenSSL through 1.0.1i s to obtain cleartext data via a			which makes it easier for	
CVE-2016-0800	https://nvd.nist.gov/vu In/detail/CVE-2016- 0800	2016-03-01	63.128.95.117	-	2018-08- 09T11:59:43.000Z
message before establishin	ed in OpenSSL before 1.0.1s and that a client possesses cering a Bleichenbacher RSA pac	tain plaintext RSA data, which	n makes it easier for remote a		
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	166.73.12.26	-	2018-08- 09T01:22:15.000Z
	sed in OpenSSL through 1.0.1i s to obtain cleartext data via a			which makes it easier for	
CVE-2015-4000	https://nvd.nist.gov/vu In/detail/CVE-2015- 4000	2015-05-20	64.149.172.137		2018-08- 08T16:20:46.000Z
DHE_EXPORT choice, which	arlier, when a DHE_EXPORT of th allows man-in-the-middle a and then rewriting a ServerH	ttackers to conduct cipher-do	owngrade attacks by rewriting	a ClientHello with DHE	
CVE-2015-0204	https://nvd.nist.gov/vu In/detail/CVE-2015- 0204	2015-01-08	64.149.172.137	-	2018-08- 08T16:20:46.000Z
	sed in OpenSSL through 1.0.1i s to obtain cleartext data via a			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	64.149.172.137	-	2018-08- 08T16:20:46.000Z
	sed in OpenSSL through 1.0.1i s to obtain cleartext data via a			which makes it easier for	
CVE-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	63.240.88.6	-	2018-07- 19T00:54:48.000Z
1.0.1m, and 1.0.2 before 1.0.	y function in s2_srvr.c in the S 2a accepts a nonzero CLIENT determine the MASTER-KEY v VE-2016-0800.	-MASTER-KEY CLEAR-KEY-L	ENGTH value for an arbitrary	cipher, which allows man-	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	63.240.88.6	-	2018-07- 19T00:54:48.000Z
lines and headers. Accepting	releases prior to 2.2.32 and 2 ng these different behaviors r olication servers, either throug ng and cache pollution.	epresented a security concer	n when httpd participates in a	any chain of proxies or	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015-	2015-07-20	208.11.141.155		2018-07- 18T20:31:47.000Z

31	83

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2015-3194

https://nvd.nist.gov/vu In/detail/CVE-20152015-12-06

208.11.141.155

2018-07-18T20:31:47.000Z

3194

Description:

crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.

CVE-2015-3195

https://nvd.nist.gov/vu In/detail/CVE-20152015-12-06

208.11.141.155

2018-07-

3195

18T20:31:47.000Z

Description:

The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.

CVE-2014-0226

https://nvd.nist.gov/vu In/detail/CVE-20142014-07-20

208.11.141.155

2018-07-

18T20:31:47.000Z

0226

Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3183

https://nvd.nist.gov/vu

2015-07-20

208.11.141.92

2018-07-

In/detail/CVE-2015-

3183

18T10:53:59.000Z

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2017-3737

https://nvd.nist.gov/vu In/detail/CVE-20172017-12-07 208.11.141.92 2018-07-

18T10:53:59.000Z

3737

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the work correctly in SSL_ready or SSL_write() is called unexpected in the antibation for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2017-3738

https://nvd.nist.gov/vu In/detail/CVE-20172017-12-07

208.11.141.92

2018-07-

18T10:53:59.000Z

3738

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2014-0226

https://nvd.nist.gov/vu

2014-07-20

208.11.141.92

2018-07-

In/detail/CVE-2014- 0226 Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua_request.c. CVE-2015-3197	9.0002					
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c. CVE-2015-3197 https://nvd.nist.gov/vu 2016-02-14 208.11.141.88 - 2018-07-1AT02:08:3 3197 Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions. CVE-2016-0703 https://nvd.nist.gov/vu 2016-03-02 208.11.141.88 - 2018-07-1AT02:08:3 Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800. CVE-2015-3194 https://nvd.nist.gov/vu 2015-12-06 208.11.141.88 - 2018-07-14T02:08:3						
In/detail/CVE-2015-3197 Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions. CVE-2016-0703						
ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions. CVE-2016-0703	2.000Z					
In/detail/CVE-2016- 0703 Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows manin-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800. CVE-2015-3194 https://nvd.nist.gov/vu 2015-12-06 208.11.141.88 - 2018-07-In/detail/CVE-2015- 14T02:08:3						
The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows manin-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800. CVE-2015-3194	52.000Z					
In/detail/CVE-2015- 14T02:08:3						
3194	2.000Z					
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.						
CVE-2015-3195 https://nvd.nist.gov/vu 2015-12-06 208.11.141.88 - 2018-07- In/detail/CVE-2015- 14T02:08:3	2.000Z					
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.						
CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.11.141.91 - 2018-07- In/detail/CVE-2017- 3738 tttps://nvd.nist.gov/vu 2017-12-07 208.11.141.91 - 2018-07- 12T18:48:43	3.000Z					
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0 when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.						
CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.91 - 2018-07- In/detail/CVE-2014- 0226 12T18:48:43						
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.	3.000Z					
CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.91 - 2018-07-12T18:48:43	3.000Z					

0	7	л	2
0	/	4	

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2017-3737

https://nvd.nist.gov/vu

2017-12-07 208.11.141.91 2018-07-

12T18:48:43.000Z

In/detail/CVE-2017-3737

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVF-2017-3736

https://nvd.nist.gov/vu

2017-11-02

208 11 141 91

2018-07-

In/detail/CVE-2017-

3736

12T18:48:43.000Z

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2015-3183

https://nvd.nist.gov/vu In/detail/CVE-20152015-07-20

208.11.141.91

2018-07-

12T18:48:43.000Z

3183

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2014-3566

https://nvd.nist.gov/vu In/detail/CVE-20142014-10-14

204.95.150.207

2018-07-

11T04:32:58.625Z

3566

Description:

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2014-3566

https://nvd.nist.gov/vu In/detail/CVE-20142014-10-14

166.73.13.26

2018-07-

3566

10T19:11:38.897Z

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2014-3566

https://nvd.nist.gov/vu

2014-10-14

209.163.213.129

2018-06-

In/detail/CVE-2014-3566

27T06:26:54.289Z

Description:

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2016-0800

https://nvd.nist.gov/vu

2016-03-01

209.163.213.129

2018-06-

In/detail/CVE-2016-0800

27T06:26:53.920Z

_						
message before establish	ed in OpenSSL before 1.0.1s a ing that a client possesses cer jing a Bleichenbacher RSA pag	tain plaintext RSA data, whicl	n makes it easier for remote a			
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	192.131.76.203	-	2018-06- 23T10:38:08.387Z	
	used in OpenSSL through 1.0.1i ers to obtain cleartext data via			which makes it easier for		
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	192.131.76.78	-	2018-06- 23T10:27:43.342Z	
	used in OpenSSL through 1.0.1i ers to obtain cleartext data via			which makes it easier for		
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	12.16.165.84	-	2018-06- 23T06:51:57.123Z	
	Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	12.16.165.238	-	2018-06- 23T05:37:48.985Z	
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.						
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	12.16.165.237	-	2018-06- 23T05:24:21.900Z	
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.						
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	12.16.165.239	-	2018-06- 23T05:17:58.401Z	
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.						
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	64.128.99.60	-	2018-06- 23T03:36:36.117Z	
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.						
			0.4.00.00.400	_	2040.00	
	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	64.128.99.136		2018-06- 23T03:25:11.211Z	
man-in-the-middle attacke CVE-2014-3566 Description: The SSL protocol 3.0, as u	In/detail/CVE-2014-	and other products, uses no	ndeterministic CBC padding,	which makes it easier for		

	In/detail/CVE-2014-				23T03:20:57.449Z			
	3566							
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.								
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	64.128.99.65	-	2018-06- 23T03:16:00.204Z			
	Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.							
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	208.31.22.6	-	2018-06- 22T22:29:12.320Z			
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for				
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	198.246.154.221	-	2018-06- 22T18:10:31.019Z			
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for				
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	166.73.13.54	-	2018-06- 22T02:31:21.737Z			
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.								
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	64.149.172.167	-	2018-06- 22T02:15:43.825Z			
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.								
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	192.131.46.150	-	2018-06- 21T01:52:19.143Z			
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.								
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	192.131.76.202		2018-06- 21T01:48:38.839Z			
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.								
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	192.131.72.207	-	2018-06- 20T20:06:33.945Z			
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.								

CVE-2014-3566 https://nvd.nist.gov/vu 2014-10-14 69.164.81.28 2018-06-In/detail/CVE-2014-20T19:52:24.454Z 3566 Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue. CVE-2015-3197 https://nvd.nist.gov/vu 2016-02-14 192.131.76.100 2018-06-In/detail/CVE-2015-20T16:30:45.000Z 3197 Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-inthe-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions. CVE-2015-3194 https://nvd.nist.gov/vu 2015-12-06 192.131.76.100 2018-06-In/detail/CVE-2015-20T16:30:45.000Z 3194 Description: crypto/rsa_rmeth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter. CVE-2014-0226 2014-07-20 192.131.76.100 https://nvd.nist.gov/vu 2018-06-In/detail/CVE-2014-20T16:30:45.000Z 0226 Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c. CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 192.131.76.100 2018-06-In/detail/CVE-2016-20T16:30:45.000Z 8743 Description: Apache HTTP Server, in all releases prior to 2,2,32 and 2,4,25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution. CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 192.131.76.100 2018-06-In/detail/CVE-2015-20T16:30:45.000Z 3185 Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior. CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 192.131.76.100 2018-06-In/detail/CVE-2015-20T16:30:45.000Z 3183 The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c. https://nvd.nist.gov/vu CVE-2015-3195 2015-12-06 192 131 76 100 2018-06-In/detail/CVE-2015-20T16:30:45.000Z Description:

The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.

CVE-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	192.131.76.100	-	2018-06- 20T16:30:45.000Z		
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows manin-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.							
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	208.235.248.122	-	2018-06- 20T15:43:02.164Z		
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for			
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	64.128.99.203	-	2018-06- 20T14:28:05.000Z		
remote attackers to condu	Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/filters.c.						
CVE-2016-0703	https://nvd.nist.gov/vu ln/detail/CVE-2016- 0703	2016-03-02	64.128.99.203	-	2018-06- 20T14:28:05.000Z		
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows manin-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.							
CVE-2015-3194	https://nvd.nist.gov/vu In/detail/CVE-2015- 3194	2015-12-06	64.128.99.203	-	2018-06- 20T14:28:05.000Z		
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.							
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	64.128.99.203	-	2018-06- 20T14:28:05.000Z		
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.							
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	64.128.99.203	-	2018-06- 20T14:28:05.000Z		
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.							
CVE-2015-3197	https://nvd.nist.gov/vu In/detail/CVE-2015- 3197	2016-02-14	64.128.99.203	-	2018-06- 20T14:28:05.000Z		
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-							

the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the $get_client_master_key$ and get_client_hello functions.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 64.128.99.203 - 2018-06-

In/detail/CVE-2015- 20T14:28:05.000Z

3185

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2015-3195 https://nvd.nist.gov/vu 2015-12-06 64.128.99.203 - 2018-06-

In/detail/CVE-2015- 20T14:28:05.000Z

3195

Description:

The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 166.73.13.244 - 2018-06-

In/detail/CVE-2014- 20T12:53:57.000Z

0226

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 166.73.13.244 - 2018-06-

In/detail/CVE-2017- 20T12:53:57.000Z

3736

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 166.73.13.244 - 2018-06-

In/detail/CVE-2017- 20T12:53:57.000Z

3737

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 166.73.13.244 - 2018-06-

In/detail/CVE-2017- 20T12:53:57.000Z

3738

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HADWARE OR DARDWARE OR HADWARE OR HA

CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	166.73.13.244	-	2018-06- 20T12:53:57.000Z
lines and headers. Accepting	releases prior to 2.2.32 and and these different behaviors rollication servers, either through and cache pollution.	epresented a security concer	n when httpd participates in a	any chain of proxies or	
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	166.73.13.244	-	2018-06- 20T12:53:57.000Z
directive may be associated	ed function in server/request. d with an authorization setting s in opportunistic circumstand	g rather than an authenticatio	n setting, which allows remot	e attackers to bypass	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	166.73.13.244	-	2018-06- 20T12:53:57.000Z
remote attackers to conduc	ng implementation in the Apa ct HTTP request smuggling at aracters in modules/http/http	tacks via a crafted request, re			
CVE-2015-3194	https://nvd.nist.gov/vu In/detail/CVE-2015- 3194	2015-12-06	64.128.99.92	-	2018-06- 20T11:36:31.000Z
	OpenSSL 1.0.1 before 1.0.1q an oplication crash) via an RSA P				
CVE-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	64.128.99.92	-	2018-06- 20T11:36:31.000Z
1.0.1m, and 1.0.2 before 1.0.	r function in s2_srvr.c in the S 2a accepts a nonzero CLIEN [*] Jetermine the MASTER-KEY v VE-2016-0800.	Γ-MASTER-KEY CLEAR-KEΥ-L	ENGTH value for an arbitrary	cipher, which allows man-	
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	64.128.99.92	-	2018-06- 20T11:36:31.000Z
(heap-based buffer overflow	_status module in the Apache w), or possibly obtain sensitiv ling within the status_handler _request.c.	e credential information or ex	ecute arbitrary code, via a cra	afted request that triggers	
CVE-2015-3195	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	64.128.99.92	-	2018-06- 20T11:36:31.000Z
1.0.2 before 1.0.2e mishand	E implementation in crypto/as dles errors caused by malform nemory by triggering a decod	ied X509_ATTRIBUTE data, v	which allows remote attackers		
CVE-2015-3197	https://nvd.nist.gov/vu In/detail/CVE-2015- 3197	2016-02-14	64.128.99.92	-	2018-06- 20T11:36:31.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.	0.1 before 1.0.1r and 1.0.2 befo	ore 1.0.2f does not prevent us	e of disabled ciphers, which i	makes it easier for man-in-	

the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the $get_client_master_key$ and get_client_hello functions.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 64.128.99.92 -

In/detail/CVE-2016-

8743

2018-06-

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 64.128.99.92 - 2018-06-

In/detail/CVE-2015-

3185

20T11:36:31.000Z

20T11:36:31.000Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 64.128.99.92 - 2018-06-

In/detail/CVE-2015-

3183

20T11:36:31.000Z

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2016-0800 https://nvd.nist.gov/vu 2016-03-01 50.58.10.133 - 2018-06-

In/detail/CVE-2016-

0800

20T07:25:52.777Z

Description:

The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.

CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 208.66.20.31 - 2018-06-

In/detail/CVE-2017-

3737

20T06:17:06.000Z

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.66.20.31 - 2018-06-

In/detail/CVE-2017-

3738

20T06:17:06.000Z

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.10-1.0.g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.66.20.31 - 2018-06-

In/detail/CVE-2017-

3736

2010-00-

20T06:17:06.000Z

19T11:26:09.000Z

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2014-3566 https://nvd.nist.gov/vu 2014-10-14 209.163.213.118 2018-06-

> In/detail/CVE-2014-20T02:09:06.653Z

3566

3566

Description:

Description:

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2014-3566 https://nvd.nist.gov/vu 2014-10-14 166.73.6.60 2018-06-

> In/detail/CVE-2014-19T21:41:08.252Z

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2014-3566 https://nvd.nist.gov/vu 208.11.141.38 2018-06-2014-10-14

> In/detail/CVE-2014-19T21:05:27.815Z

3566

Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2014-3566 https://nvd.nist.gov/vu 2014-10-14 63.128.95.117 2018-06-

> In/detail/CVE-2014-19T17:51:01.888Z

3566

Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

2018-06-

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 166.73.6.118

3736

In/detail/CVE-2017-

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 166.73.6.117 2018-06-In/detail/CVE-2017-19T11:25:05.000Z

3737

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 166.73.6.117 2018-06-19T11:25:05.000Z

In/detail/CVE-2015-

3183

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 166.73.6.117 2018-06-

In/detail/CVE-2017-19T11:25:05.000Z

3738

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.11.141.92 2018-06-

In/detail/CVE-2017-

3736

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.92 2018-06-

In/detail/CVE-2016-

8743

19T11:08:41.000Z

19T11:08:41.000Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.92 2018-06-

In/detail/CVE-2015-

3185

19T11:08:41.000Z

Description:

The an_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.11.141.75 2018-06-

In/detail/CVE-2015-

3183

19T11:08:30.000Z

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.75 2018-06-

In/detail/CVE-2016-

19T11:08:30.000Z

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.177 2018-06-

In/detail/CVE-2015-

3185

19T11:04:01.000Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2015-3185

https://nvd.nist.gov/vu In/detail/CVE-2015-

2015-07-20

208.11.141.78

2018-06-19T10:55:59.000Z

3185

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2017-3736

https://nvd.nist.gov/vu 2017-11-02 208 11 141 78

2018-06-

19T10:55:59.000Z

In/detail/CVE-2017-

3736

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2016-8743

https://nvd.nist.gov/vu In/detail/CVE-20162017-07-27

208.11.141.78

2018-06-

19T10:55:59.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2014-0226

https://nvd.nist.gov/vu 2014-07-20 In/detail/CVE-2014208.11.141.78

2018-06-

19T10:55:59.000Z

0226

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3738

https://nvd.nist.gov/vu In/detail/CVE-20172017-12-07

208.11.141.78

2018-06-

19T10:55:59.000Z

3738

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2015-3183

https://nvd.nist.gov/vu In/detail/CVE-2015-

3183

2015-07-20

208.11.141.78

2018-06-

19T10:55:59.000Z

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2017-3737

https://nvd.nist.gov/vu 2017-12-07 208.11.141.78

2018-06-

In/detail/CVE-2017-19T10:55:59.000Z 3737

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208 11 141 155 2018-06-

> 19T05:25:46.000Z In/detail/CVE-2015-

3185

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208 11 141 155 2018-06-

> In/detail/CVE-2016-19T05:25:46.000Z

8743

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2016-0703 https://nvd.nist.gov/vu 2016-03-02 208.11.141.155 2018-06-

> In/detail/CVE-2016-19T05:25:46.000Z

0703

Description:

The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows manin-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

CVE-2015-3197 https://nvd.nist.gov/vu 2016-02-14 208.11.141.155 2018-06-

> In/detail/CVE-2015-19T05:25:46.000Z

3197

Description:

ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-inthe-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.

CVE-2017-5647 https://nvd.nist.gov/vu 2017-04-17 198.167.0.17 2018-06-

In/detail/CVE-2017-19T03:03:57.000Z

5647

Description:

A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 166.73.14.117 2018-06-

In/detail/CVE-2017-

3738

19T02:47:08.000Z

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be

included in OpenSSL 1.1.0h	n when it becomes available. T	he fix is also available in com	nmit e502cc86d in the OpenS	SSL git repository.	
CVE-2017-3736	https://nvd.nist.gov/vu In/detail/CVE-2017- 3736	2017-11-02	166.73.14.117	-	2018-06- 19T02:47:08.000Z
algorithms are affected. Ar are not believed likely. Attainformation about a private likely only accessible to a target private key in a scer	ng bug in the x86_64 Montgor nalysis suggests that attacks a acks against DH are considere e key may be performed offline limited number of attackers. A nario with persistent DH paran e BMI1, BMI2 and ADX extens	gainst RSA and DSA as a reset just feasible (although very e. The amount of resources re n attacker would additionally neters and a private key that	ult of this defect would be ver difficult) because most of the equired for such an attack wo need online access to an ung s shared between multiple cl	ry difficult to perform and e work necessary to deduce ould be very significant and patched system using the ients. This only affects	
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	166.73.14.117	-	2018-06- 19T02:47:08.000Z
(heap-based buffer overflo	_status module in the Apache ow), or possibly obtain sensitive lling within the status_handler a_request.c.	e credential information or ex	ecute arbitrary code, via a cra	afted request that triggers	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	209.163.213.129	-	2018-06- 19T02:23:01.233Z
	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via a			which makes it easier for	
CVE-2016-0800	https://nvd.nist.gov/vu In/detail/CVE-2016- 0800	2016-03-01	209.163.213.129	-	2018-06- 19T02:23:00.878Z
message before establishi	ed in OpenSSL before 1.0.1s ar ing that a client possesses cer ing a Bleichenbacher RSA pac	tain plaintext RSA data, which	n makes it easier for remote a		
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	209.163.213.130	-	2018-06- 19T02:17:39.014Z
	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via a			which makes it easier for	
CVE-2016-0800	https://nvd.nist.gov/vu In/detail/CVE-2016- 0800	2016-03-01	209.163.213.130	-	2018-06- 19T02:17:38.652Z
message before establishi	ed in OpenSSL before 1.0.1s ai ing that a client possesses cer ing a Bleichenbacher RSA pac	tain plaintext RSA data, which	n makes it easier for remote a		
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	209.163.213.138	-	2018-06- 19T02:13:18.076Z
	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via a			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	208.235.248.43	-	2018-06- 19T01:54:47.200Z

	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	64.128.99.48	-	2018-06- 19T01:45:22.193Z
	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	64.128.99.68	-	2018-06- 19T00:06:33.740Z
	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	198.246.154.136		2018-06- 18T22:50:07.203Z
	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	209.163.213.170		2018-06- 18T22:00:04.797Z
	sed in OpenSSL through 1.0.1i rs to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	69.164.81.29	-	2018-06- 18T21:09:37.575Z
	sed in OpenSSL through 1.0.1i			which makes it easier for	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	64.149.172.137	-	2018-06- 18T18:20:08.000Z
lines and headers. Accepti	I releases prior to 2.2.32 and a ling these different behaviors replication servers, either throughing and cache pollution.	epresented a security conce	rn when httpd participates in	any chain of proxies or	
CVE-2017-5647	https://nvd.nist.gov/vu In/detail/CVE-2017- 5647	2017-04-17	192.131.72.236	-	2018-06- 18T16:50:16.000Z
and 6.0.0 to 6.0.52, when completed. This could resu	ne pipelined requests in Apach send file was used, results in ult in responses appearing to I sponse for request A, the resp	the pipelined request being lobe sent for the wrong reques	ost when send file processing t. For example, a user agent t	g of the previous request hat sent requests A, B and	
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	192.131.72.203	-	2018-06- 18T16:42:46.000Z
	_status module in the Apache w), or possibly obtain sensitiv				

improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 192.131.72.203 2018-06-

18T16:42:46.000Z In/detail/CVE-2015-

3185

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

208.11.141.91 CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 2018-06-

In/detail/CVE-2014-

0226

18T15:45:34.000Z

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 208 11 141 91 2018-06-

In/detail/CVE-2017-

3737

18T15:45:34.000Z

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.91 2018-06-In/detail/CVE-2015-

3185

18T15:45:34.000Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.11.141.91 2018-06-

In/detail/CVE-2015-

3183

18T15:45:34.000Z

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2015-3197 https://nvd.nist.gov/vu 2016-02-14 208.11.141.88 2018-06-

In/detail/CVE-2015-

3197

18T15:37:06.000Z

Description:

ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-inthe-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.

208.11.141.88 CVE-2014-0226 https://nvd.nist.gov/vu 2018-06-2014-07-20

In/detail/CVE-2014-

0226

18T15:37:06.000Z

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2016-0703 https://nvd.nist.gov/vu 2016-03-02 208.11.141.88 2018-06-In/detail/CVE-2016-18T15:37:06.000Z 0703 Description: The get_client_master_key function in s2_sryr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 10.1m, and 10.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800. CVE-2015-3194 https://nvd.nist.gov/vu 2015-12-06 208.11.141.88 2018-06-In/detail/CVE-2015-18T15:37:06.000Z 3194 Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter. CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.88 2018-06-In/detail/CVE-2016-18T15:37:06.000Z 8743 Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution. CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.88 2018-06-In/detail/CVE-2015-18T15:37:06.000Z 3185 Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior. CVF-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.11.141.88 2018-06-In/detail/CVE-2015-18T15:37:06.000Z 3183 The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c. CVE-2015-3195 https://nvd.nist.gov/vu 208.11.141.88 2018-06-2015-12-06 In/detail/CVE-2015-18T15:37:06.000Z 3195 Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application. CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.76 2018-06-In/detail/CVE-2014-18T15:37:03.000Z 0226 Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c. CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 208.11.141.76 2018-06-In/detail/CVE-2017-18T15:37:03.000Z 3737 Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a

handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.76 2018-06-

In/detail/CVE-2016-18T15:37:03.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2,2,32 and 2,4,25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.11.141.76 2018-06-

In/detail/CVE-2015-18T15:37:03.000Z

3183

Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and

CVF-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208 11 141 76 2018-06-

In/detail/CVE-2017-18T15:37:03.000Z

3736

invalid chunk-extension characters in modules/http/http_filters.c.

Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce

information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.11.141.76 2018-06-

In/detail/CVE-2017-18T15:37:03.000Z

3738

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

2018-06-CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.76 In/detail/CVE-2015-18T15:37:03.000Z

3185

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.11.141.196 2018-06-18T14:04:53.000Z

In/detail/CVE-2015-

3183

Description:

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208 11 141 196 2018-06-18T14:04:53.000Z In/detail/CVE-2014-Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c. CVE-2015-3197 https://nvd.nist.gov/vu 2016-02-14 208.11.141.196 2018-06-In/detail/CVE-2015-18T14:04:53.000Z 3197 Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-inthe-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions. CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.196 2018-06-In/detail/CVE-2016-18T14:04:53.000Z 8743 Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution. https://nvd.nist.gov/vu CVE-2015-3194 2015-12-06 208.11.141.196 2018-06-In/detail/CVE-2015-18T14:04:53.000Z 3194 Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter. CVE-2016-0703 https://nvd.nist.gov/vu 2016-03-02 208.11.141.196 2018-06-In/detail/CVE-2016-18T14:04:53.000Z 0703 Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows manin-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800. CVE-2015-3195 https://nvd.nist.gov/vu 2015-12-06 208.11.141.196 2018-06-In/detail/CVE-2015-18T14:04:53.000Z 3195 Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application. CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.196 2018-06-In/detail/CVE-2015-18T14:04:53.000Z 3185 Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior. CVE-2015-3195 https://nvd.nist.gov/vu 2015-12-06 208.11.141.167 2018-06-In/detail/CVE-2015-18T14:03:31.000Z 3195 Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HADWARE OR DARDWARE OR HADWARE OR HA

	https://nvd.nist.gov/vu In/detail/CVE-2015-	2015-12-06	208.11.141.167		2040.00
	,	2015-12-06	208 11 141 167		2040.00
	3194		200.11.141.107	-	2018-06- 18T14:03:31.000Z
			emote attackers to cause a de a mask generation function p		
	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	208.11.141.167	-	2018-06- 18T14:03:31.000Z
directive may be associated	with an authorization setting	rather than an authentication	2.4.x before 2.4.14 does not on setting, which allows remote of a module that relies on t	e attackers to bypass	
	https://nvd.nist.gov/vu In/detail/CVE-2015- 3197	2016-02-14	208.11.141.167	-	2018-06- 18T14:03:31.000Z
	at cryptographic protection i		e of disabled ciphers, which romputations on SSLv2 traffic,		
	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	208.11.141.167	-	2018-06- 18T14:03:31.000Z
1.0.1m, and 1.0.2 before 1.0.2a	a accepts a nonzero CLIENT etermine the MASTER-KEY v	-MASTER-KEY CLEAR-KEY-L	nSSL before 0.9.8zf, 1.0.0 bef ENGTH value for an arbitrary ext data by leveraging a Bleic	cipher, which allows man-	
	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	208.11.141.167	-	2018-06- 18T14:03:31.000Z
	HTTP request smuggling at	tacks via a crafted request, re	4 does not properly parse ch elated to mishandling of large		
	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	208.11.141.167	-	2018-06- 18T14:03:31.000Z
(heap-based buffer overflow)), or possibly obtain sensitiveng within the status_handler	e credential information or ex	llows remote attackers to cau ecute arbitrary code, via a cra ors/mod_status.c and the lua	afted request that triggers	
	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	209.163.213.137	-	2018-06- 18T13:13:54.691Z
		and other products, uses nor a padding-oracle attack, aka t	ndeterministic CBC padding, \ he "POODLE" issue.	which makes it easier for	
	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	208.235.248.231	-	2018-06- 18T12:26:57.000Z
Description: The ASN1_TFLG_COMBINE i	implementation in crypto/as	n1/tasn_dec.c in OpenSSL be	fore 0.9.8zh, 1.0.0 before 1.0.	Ot, 1.0.1 before 1.0.1q, and	

VE-2014-0226	https://nvd.nist.gov/vu	2014-07-20	208.235.248.231	-	2018-06-
VE 2011 0220	In/detail/CVE-2014- 0226	2011 07 20	200.200.2 10.201		18T12:26:57.000Z
eap-based buffer ove	rflow), or possibly obtain sensitivendling within the status_handler	e credential information	4.10 allows remote attackers to ca or execute arbitrary code, via a c enerators/mod_status.c and the lu	crafted request that triggers	
VE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	208.235.248.231	-	2018-06- 18T12:26:57.000Z
mote attackers to con		tacks via a crafted requ	e 2.4.14 does not properly parse clest, related to mishandling of larg		
/E-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	208.235.248.231	-	2018-06- 18T12:26:57.000Z
.1m, and 1.0.2 before	1.0.2a accepts a nonzero CLIEN to determine the MASTER-KEY v	Γ-MASTER-KEY CLEAR-	n OpenSSL before 0.9.8zf, 1.0.0 bo KEY-LENGTH value for an arbitrar iphertext data by leveraging a Ble	y cipher, which allows man-	
/E-2015-3194	https://nvd.nist.gov/vu In/detail/CVE-2015- 3194	2015-12-06	208.235.248.231	-	2018-06- 18T12:26:57.000Z
			ows remote attackers to cause a lacks a mask generation function		
/E-2015-3197	https://nvd.nist.gov/vu In/detail/CVE-2015- 3197	2016-02-14	208.235.248.231	-	2018-06- 18T12:26:57.000Z
e-middle attackers to			ent use of disabled ciphers, which ning computations on SSLv2 traffi		
/E-2015-3195	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	64.149.172.15	-	2018-06- 18T11:44:43.000Z
.2 before 1.0.2e mish		ed X509_ATTRIBUTE	SSL before 0.9.8zh, 1.0.0 before 1.data, which allows remote attacke or CMS application.		
/E-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	64.149.172.15		2018-06- 18T11:44:43.000Z
ective may be associ	ated with an authorization setting	g rather than an authen	Server 2.4.x before 2.4.14 does no tication setting, which allows remo resence of a module that relies or	ote attackers to bypass	
/E-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016-	2016-03-02	64.149.172.15	-	2018-06- 18T11:44:43.000Z

18T11:44:43.000Z

18T08:40:28.805Z

D	
Descri	

The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows manin-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 64.149.172.15

2018-06-In/detail/CVE-2016-18T11:44:43.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3197 https://nvd.nist.gov/vu 64.149.172.15 2016-02-14 2018-06-

> In/detail/CVE-2015-18T11:44:43.000Z

3197

Description:

ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-inthe-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.

CVE-2014-0226 2018-06https://nvd.nist.gov/vu 2014-07-20 64.149.172.15

In/detail/CVE-2014-18T11:44:43.000Z

0226

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3194 https://nvd.nist.gov/vu 2015-12-06 64.149.172.15 2018-06-

In/detail/CVE-2015-18T11:44:43.000Z

3194

Description:

crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 64.149.172.15 2018-06-

In/detail/CVE-2015-

Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and

invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2016-0800 https://nvd.nist.gov/vu 2016-03-01 205.219.236.229 2018-06-

In/detail/CVE-2016-

0800

18T11:35:59.907Z

The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.

CVE-2014-3566 https://nvd.nist.gov/vu 2018-06-2014-10-14 12.16.164.210

In/detail/CVE-2014-

3566

Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2014-3566 https://nvd.nist.gov/vu 2014-10-14 12.16.165.142 2018-06-

In/detail/CVE-2014-18T04:22:17.241Z

	3566				
	3300				
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	12.16.165.109	-	2018-06- 18T03:42:52.313Z
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	12.16.165.87	-	2018-06- 18T03:35:29.240Z
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for	
CVE-2015-4000	https://nvd.nist.gov/vu In/detail/CVE-2015- 4000	2015-05-20	12.16.165.87	-	2018-06- 18T03:35:29.240Z
DHE_EXPORT choice, wh	earlier, when a DHE_EXPORT nich allows man-in-the-middle a IT and then rewriting a Serverl	nttackers to conduct cipher-do	owngrade attacks by rewriting	g a ClientHello with DHE	
CVE-2015-0204	https://nvd.nist.gov/vu In/detail/CVE-2015- 0204	2015-01-08	12.16.165.87	-	2018-06- 18T03:35:29.239Z
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	204.95.150.210	-	2018-06- 17T20:11:19.550Z
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	204.95.150.200	-	2018-06- 17T20:00:13.871Z
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for	
CVE-2015-0204	https://nvd.nist.gov/vu In/detail/CVE-2015- 0204	2015-01-08	204.95.150.47	-	2018-06- 17T17:28:08.735Z
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for	
CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	208.31.22.1	-	2018-06- 16T23:13:47.875Z
	used in OpenSSL through 1.0.1 ers to obtain cleartext data via			which makes it easier for	

CVE-2014-3566	https://nvd.nist.gov/vu In/detail/CVE-2014- 3566	2014-10-14	12.44.79.219	-	2018-06- 16T20:01:11.921Z
	used in OpenSSL through 1.0.1i ers to obtain cleartext data via			which makes it easier for	
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	208.11.141.155	-	2018-06- 13T20:31:22.000Z
directive may be associat	ired function in server/request. ed with an authorization settin ons in opportunistic circumstan	g rather than an authenticatio	n setting, which allows remot	e attackers to bypass	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	208.11.141.155	-	2018-06- 13T20:31:22.000Z
lines and headers. Accept	all releases prior to 2.2.32 and ting these different behaviors i pplication servers, either through ting and cache pollution.	represented a security conce	rn when httpd participates in	any chain of proxies or	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	208.11.141.155	-	2018-06- 13T20:31:22.000Z
remote attackers to condi	ling implementation in the Apa uct HTTP request smuggling at haracters in modules/http/http.	ttacks via a crafted request, r			
CVE-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	208.11.141.155	-	2018-06- 13T20:31:22.000Z
1.0.1m, and 1.0.2 before 1.0	ey function in s2_srvr.c in the S 0.2a accepts a nonzero CLIEN' determine the MASTER-KEY v CVE-2016-0800.	T-MASTER-KEY CLEAR-KEY-L	ENGTH value for an arbitrary	cipher, which allows man-	
CVE-2015-3194	https://nvd.nist.gov/vu In/detail/CVE-2015- 3194	2015-12-06	208.11.141.155	-	2018-06- 13T20:31:22.000Z
	OpenSSL 1.0.1 before 1.0.1q ar application crash) via an RSA P				
CVE-2015-3195	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	208.11.141.155	-	2018-06- 13T20:31:22.000Z
1.0.2 before 1.0.2e mishar	NE implementation in crypto/as ndles errors caused by malform memory by triggering a decod	ned X509_ATTRIBUTE data,	which allows remote attackers		
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	208.11.141.155	-	2018-06- 13T20:31:22.000Z
(heap-based buffer overfl-	d_status module in the Apache ow), or possibly obtain sensitiv dling within the status_handler	e credential information or ex	ecute arbitrary code, via a cr	afted request that triggers	

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PUPPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

function in modules/lua/lua_request.c.

CVE 2015-3197 Intersection of the province of						
salad_serve in OpureSt. 101 before 10.8 med 10.2 before 10.2 does not prevent use of disabled ciphers, which makes it tender for man in the-middle absoration to delete cryptopring protection mechanisms by performing computations on SSLV2 treffir, related to the general common protection on Section 10 per 10 p	CVE-2015-3197	In/detail/CVE-2015-	2016-02-14	208.11.141.155	-	
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response interest and the prior to the prior to 1.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response or large and the prior to 1.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response and prior to 1.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response in the prior to 1.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response in large and the prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response in large and the prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response in large and the prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response in large and the prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response in large and the prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response in large and the large and the prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response in large and the large and t	ssl/s2_srvr.c in OpenSSL the-middle attackers to de	efeat cryptographic protection				
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response internds with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request amaging in the propose pollution. CVE-2016-8743 https://mvd.nist.gov/vu 2017-07-27 198.167.0.246 - 2018-06-3714.42.16.0002 Discoplinar internds with proxy or the proxy or using conventional CGI mechanisms, and may result in request and sent in response internds with proxy or using conventional CGI mechanisms, and may result in request and sent in response internds with backer and application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or internds with backer application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution. CVE-2015-3185 https://rud.nist.gov/vu 2015-07-20 208.11.141.91 - 2018-06-12714.33.32.000Z 3185 Discoplinar Di	CVE-2016-8743	In/detail/CVE-2016-	2017-07-27	198.167.0.17	-	
Invidetal/CVE-2016-8/743 Invidence I	Apache HTTP Server, in a lines and headers. Accept interacts with back-end appropriate to the server of the server	ting these different behaviors i oplication servers, either throu	represented a security conce	rn when httpd participates in	any chain of proxies or	
Apache HTTP Server, in all releases prior to 2,232 and 2,425, was liberal in the whitespace accepted from requests and sent in response interacts. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response spilithing and cache pollution. CVE-2015-3185	CVE-2016-8743	In/detail/CVE-2016-	2017-07-27	198.167.0.246	-	
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior. CVE-2016-0703	Apache HTTP Server, in a lines and headers. Accept interacts with back-end approximately approximate	ting these different behaviors i oplication servers, either throu	represented a security conce	rn when httpd participates in	any chain of proxies or	
The ap_some_auth_required function in server/requests in the Apache HTTP Server 2.4x before 2.4/14 does not consider that a Require directive may be associated with an authorization setting rather than an autherization setting. which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior. CVE-2016-0703 https://nvd.nist.gov/vu In/detail/CVE-2016-0703 https://nvd.nist.gov/vu In/detail/CVE-2016-0703 Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1r, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800. CVE-2015-3194 https://nvd.nist.gov/vu In/detail/CVE-2015-3194 https://nvd.nist.gov/vu In/detail/CVE-2015-3194 Description: crypto/ssa/sa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN1 signature that tacks a mask generation function parameter. CVE-2015-3185 https://nvd.nist.gov/vu In/detail/CVE-2015-3185 https://nvd.nist.gov/vu In/detail/CVE-2015-3185 https://nvd.nist.gov/vu In/detail/CVE-2015-3183 https://nvd.nist.gov/vu In/detail/CVE-2015-3183 https://nvd.nist.gov/vu In/detail/CVE-2015-3183 https://nvd.nist.gov/vu In/detail/CVE-2015-3183	CVE-2015-3185	In/detail/CVE-2015-	2015-07-20	208.11.141.91	-	
In/detail/CVE-2016- 0703	The ap_some_auth_requ directive may be associat	ed with an authorization setting	g rather than an authenticatio	n setting, which allows remot	e attackers to bypass	
The get_client_master_key function in s2_srvr_c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 10.0 before 1.0.0r, 1.0.1 before 1.0.0r, 1.0.1 before 1.0.2 accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows manin-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800. CVE-2015-3194	CVE-2016-0703	In/detail/CVE-2016-	2016-03-02	208.11.141.73	-	
In/detail/CVE-2015-3194 Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter. CVE-2015-3185	The get_client_master_ke 1.0.1m, and 1.0.2 before 1.0 in-the-middle attackers to	0.2a accepts a nonzero CLIEN determine the MASTER-KEY v	T-MASTER-KEY CLEAR-KEY-L	ENGTH value for an arbitrary	cipher, which allows man-	
crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter. CVE-2015-3185	CVE-2015-3194	In/detail/CVE-2015-	2015-12-06	208.11.141.73	-	
In/detail/CVE-2015-3185 Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior. CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 166.73.13.27 - 2018-05-1n/detail/CVE-2015-3183	crypto/rsa/rsa_ameth.c in					
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior. CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 166.73.13.27 - 2018-05- In/detail/CVE-2015- 3183 2015-07-20 2015-07-2	CVE-2015-3185	In/detail/CVE-2015-	2015-07-20	208.11.141.73	-	
In/detail/CVE-2015- 20T05:35:39.000Z 3183	The ap_some_auth_requ directive may be associat	ed with an authorization setting	g rather than an authenticatio	n setting, which allows remot	e attackers to bypass	
Description:	CVE-2015-3183	In/detail/CVE-2015-	2015-07-20	166.73.13.27	-	
	Description:					

remote attackers to conduc	ng implementation in the Apac ct HTTP request smuggling at aracters in modules/http/http_	tacks via a crafted request, re		•	
CVE-2014-0226	https://nvd.nist.gov/vu ln/detail/CVE-2014- 0226	2014-07-20	192.131.72.203	-	2018-05- 20T05:35:39.000Z
(heap-based buffer overflow	_status module in the Apache w), or possibly obtain sensitiv ling within the status_handler _request.c.	e credential information or ex	ecute arbitrary code, via a cra	afted request that triggers	
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	192.131.76.193	-	2018-05- 20T05:35:39.000Z
(heap-based buffer overflow	_status module in the Apache w), or possibly obtain sensitiv ling within the status_handler ı_request.c.	e credential information or ex	ecute arbitrary code, via a cra	afted request that triggers	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	192.131.72.203	-	2018-05- 20T05:35:39.000Z
remote attackers to conduc	ng implementation in the Apar ct HTTP request smuggling at aracters in modules/http/http_	tacks via a crafted request, re			
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	166.73.13.27	-	2018-05- 20T05:35:39.000Z
directive may be associate	ed function in server/request. d with an authorization setting is in opportunistic circumstand	rather than an authenticatio	n setting, which allows remot	e attackers to bypass	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	166.73.6.118	-	2018-05- 20T05:35:39.000Z
remote attackers to conduc	ng implementation in the Aparct HTTP request smuggling at aracters in modules/http/http_	tacks via a crafted request, re	4 does not properly parse ch elated to mishandling of large	unk headers, which allows chunk-size values and	
CVE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	208.66.20.31	-	2018-05- 20T05:35:39.000Z
handshake then OpenSSL as designed for the explicit work correctly if SSL_read(initial function call. If SSL_r is passed without being de have to be present that res	m version 1.0.2b) introduced a would move into the error stat thandshake functions (SSL_d) or SSL_write() is called directed()/SSL_write() is subseque crypted/encrypted directly frosulted in a call to SSL_read()/SFixed in OpenSSL 1.0.2n. Opens	te and would immediately fai o_handshake(), SSL_accept() tly. In that scenario, if the han ntly called by the application im the SSL/TLS record layer. SL_write() being issued after	I if you attempted to continue and SSL_connect()), howeve dshake fails then a fatal error for the same SSL object then In order to exploit this issue a	the handshake. This works r due to a bug it does not r will be returned in the it will succeed and the data in application bug would	
CVE-2017-3738	https://nvd.nist.gov/vu In/detail/CVE-2017- 3738	2017-12-07	208.66.20.31	-	2018-05- 20T05:35:39.000Z
are affected. Analysis sugg	n the AVX2 Montgomery multi jests that attacks against RSA ainst DH1024 are considered j	and DSA as a result of this de	efect would be very difficult to	perform and are not	

private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2016-8743

https://nvd.nist.gov/vu ln/detail/CVE-20162017-07-27

198.167.0.48

2018-05-

20T05:35:39.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2016-8743

https://nvd.nist.gov/vu

2017-07-27

198.167.0.133

2018-05-

In/detail/CVE-2016-

8743

20T05:35:39.000Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3185

https://nvd.nist.gov/vu In/detail/CVE-20152015-07-20

166 73 6 118

2018-05-

20T05:35:39.000Z

3185

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2016-8743

https://nvd.nist.gov/vu 2017-07-27 In/detail/CVE-2016198.167.0.246

2018-05-

20T05:35:39.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2014-0226

https://nvd.nist.gov/vu In/detail/CVE-20142014-07-20

166.73.13.27

2018-05-

20T05:35:39.000Z

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3737

https://nvd.nist.gov/vu In/detail/CVE-2017-

2017-12-07

166.73.6.118

2018-05-

20T05:35:39.000Z

3737

0226

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the intention call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2016-8743

https://nvd.nist.gov/vu In/detail/CVE-20162017-07-27

192.131.55.83

2018-05-

20T05:35:39.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2014-0226

https://nvd.nist.gov/vu In/detail/CVE-20142014-07-20

64.128.99.92

2018-05-20T05:35:39.000Z

0226

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2016-8743

https://nvd.nist.gov/vu

2017-07-27

198.167.0.17

2018-05-

In/detail/CVE-2016-

8743

20T05:35:39.000Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2017-3736

https://nvd.nist.gov/vu

2017-11-02

166.73.13.27

2018-05-

In/detail/CVE-2017-

3736

20T05:35:39.000Z

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2015-3183

https://nvd.nist.gov/vu In/detail/CVE-20152015-07-20

2017-07-27

192.131.76.193

2018-05-

20T05:35:39.000Z

3183

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/filters.c.

CVE-2016-8743

https://nvd.nist.gov/vu In/detail/CVE-2016-

In/detail/CVE-2017-

198.167.0.148

2018-05-

20T05:35:39.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2017-3737

https://nvd.nist.gov/vu 2017-12-07

192.131.55.83

2018-05-

20T05:35:39.000Z

3737

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2014-0226

https://nvd.nist.gov/vu

2014-07-20

192.131.76.100

2018-05-

	In/detail/CVE-2014- 0226				20T05:35:39.000Z
(heap-based buffer overflo	d_status module in the Apache ow), or possibly obtain sensitiv dling within the status_handler a_request.c.	e credential information or ex	ecute arbitrary code, via a cr	afted request that triggers	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	192.131.76.100	-	2018-05- 20T05:35:39.000Z
lines and headers. Accept	Ill releases prior to 2.2.32 and 2 ting these different behaviors r oplication servers, either through ting and cache pollution.	epresented a security concer	n when httpd participates in	any chain of proxies or	
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	192.131.76.100	-	2018-05- 20T05:35:39.000Z
directive may be associate	ired function in server/request. ed with an authorization setting ns in opportunistic circumstand	rather than an authenticatio	n setting, which allows remot	e attackers to bypass	
CVE-2017-3738	https://nvd.nist.gov/vu In/detail/CVE-2017- 3738	2017-12-07	166.73.6.118	-	2018-05- 20T05:35:39.000Z
are affected. Analysis sug- believed likely. Attacks ag private key may be perfor TLS to be meaningful, the 2016-0701. This only affect from this issue is similar to Fixed in OpenSSL 1.0.2n. I	in the AVX2 Montgomery multi gests that attacks against RSA gainst DH1024 are considered j med offline. The amount of res server would have to share th this processors that support the o CVE-2017-3736, CVE-2017-37 Due to the low severity of this h when it becomes available. T	and DSA as a result of this do ust feasible, because most of ources required for such an a e DH1024 private key among AVX2 but not ADX extensior 32 and CVE-2015-3193. Oper ssue we are not issuing a nevent	efect would be very difficult to the work necessary to dedunattack would be significant. Homeling in the significant would be significant to multiple clients, which is not so like Intel Haswell (4th genenature) and work release of OpenSSL 1.1.0 are workers.	o perform and are not ce information about a lowever, for an attack on longer an option since CVE-cration). Note: The impact d 1.1.0-1.1.0g are affected. It this time. The fix will be	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	166.73.13.27	-	2018-05- 20T05:35:39.000Z
lines and headers. Accept	ill releases prior to 2.2.32 and 2 ting these different behaviors r oplication servers, either through ting and cache pollution.	epresented a security concer	n when httpd participates in	any chain of proxies or	
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	192.131.72.203	-	2018-05- 20T05:35:39.000Z
lines and headers. Accept	Ill releases prior to 2.2.32 and 2 ting these different behaviors r oplication servers, either through ting and cache pollution.	epresented a security concer	n when httpd participates in	any chain of proxies or	
CVE-2017-3737	https://nvd.nist.gov/vu In/detail/CVE-2017- 3737	2017-12-07	192.131.55.82	-	2018-05- 20T05:35:39.000Z
handshake then OpenSSL as designed for the explic work correctly if SSL_reac	om version 1.0.2b) introduced a would move into the error sta cit handshake functions (SSL_d d() or SSL_write() is called direc read()/SSL_write() is subseque	te and would immediately fai o_handshake(), SSL_accept() tly. In that scenario, if the han	l if you attempted to continue and SSL_connect()), howeve idshake fails then a fatal erro	e the handshake. This works or due to a bug it does not r will be returned in the	

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PUPPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data

is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would
have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version
1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 166.73.6.118 2018-05-In/detail/CVE-2016-20T05:35:39.000Z 8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2016-8743 https://nvd.nist.gov/vu 2018-05-2017-07-27 192.131.76.193

In/detail/CVE-2016-

8743

20T05:35:39.000Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 192 131 72 203 2018-05-

In/detail/CVE-2015-

3185

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2017-3738 2017-12-07 192.131.55.82 2018-05https://nvd.nist.gov/vu

In/detail/CVE-2017-

3738

20T05:35:39.000Z

20T05:35:39.000Z

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

https://nvd.nist.gov/vu CVE-2016-8743 2017-07-27 198.167.0.248 2018-05-

In/detail/CVE-2016-

8743

20T05:35:39.000Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

https://nvd.nist.gov/vu CVE-2017-3736 2017-11-02 192.131.55.82 2018-05-

In/detail/CVE-2017-

3736

20T05:35:39.000Z

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 2018-05-

In/detail/CVE-2015-

192.131.76.100

20T05:35:39.000Z

3183

3736

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2017-3736

https://nvd.nist.gov/vu

2017-11-02

166.73.6.118

2018-05-

In/detail/CVE-2017-

00.70.0.110

20T05:35:39.000Z

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVF-2016-8743

https://nvd.nist.gov/vu In/detail/CVE-20162017-07-27

198.167.0.33

2018-05-

20T05:35:39.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2017-3737

https://nvd.nist.gov/vu In/detail/CVE-20172017-12-07

166.73.13.27

2018-05-

20T05:35:39.000Z

3737

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2017-3736

https://nvd.nist.gov/vu In/detail/CVE-20172017-11-02

208.66.20.31

2018-05-

20T05:35:39.000Z

3736

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2016-8743

https://nvd.nist.gov/vu 2017-07-27 In/detail/CVE-201663.240.88.6

2018-05-

20T05:35:39.000Z

8743

3738

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2017-3738

https://nvd.nist.gov/vu In/detail/CVE-20172017-12-07

166.73.13.27

2018-05-

20T05:35:39.000Z

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms

are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 192.131.55.82 2018-05-In/detail/CVE-2016-20T05:35:39.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

https://nvd.nist.gov/vu CVE-2017-3736 2017-11-02 192.131.55.83 2018-05-

> In/detail/CVE-2017-20T05:35:39.000Z

3736

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 192.131.55.83 2018-05-

In/detail/CVE-2017-20T05:35:39.000Z

3738

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation), Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 192.131.76.193 2018-05-

In/detail/CVE-2015-

3185

20T05:35:39.000Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 166.73.6.118 2018-05-

In/detail/CVE-2014-

0226

20T05:35:39.000Z

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 64.149.172.15 2018-05-

> In/detail/CVE-2016-20T01:09:32.000Z

8743

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request

smuggling, response splitting and cache pollution. CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 64.149.172.137 2018-05-20T01:09:32.000Z In/detail/CVE-2016-8743 Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution. CVE-2015-3195 https://nvd.nist.gov/vu 2015-12-06 64.149.172.15 2018-05-In/detail/CVE-2015-20T00:51:30.000Z 3195 Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application. CVF-2015-3185 https://nvd.nist.gov/vu 2015-07-20 64 149 172 15 2018-05-In/detail/CVE-2015-20T00:51:30.000Z 3185 Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior. CVE-2016-0703 https://nvd.nist.gov/vu 2016-03-02 64.149.172.15 2018-05-In/detail/CVE-2016-20T00:51:30.000Z 0703 Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows manin-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800. CVE-2015-3197 https://nvd.nist.gov/vu 2016-02-14 64.149.172.15 2018-05-In/detail/CVE-2015-20T00:51:30.000Z 3197 Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-inthe-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions. CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 64.149.172.15 2018-05-In/detail/CVE-2014-20T00:51:30.000Z 0226 Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker

function in modules/lua/lua_request.c.

CVE-2015-3194 https://nvd.nist.gov/vu 2015-12-06 64.149.172.15 2018-05-

In/detail/CVE-2015-20T00:51:30.000Z

3194

Description:

crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.

CVE-2015-3183 2018-05https://nvd.nist.gov/vu 2015-07-20 64.149.172.15

In/detail/CVE-2015-

20T00:51:30.000Z 3183

Description:

remote attackers to condu	ing implementation in the Apa uct HTTP request smuggling at naracters in modules/http/http_	tacks via a crafted request, r			
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	64.128.99.203	-	2018-05- 20T00:10:03.000Z
lines and headers. Accept	II releases prior to 2.2.32 and a ring these different behaviors r pplication servers, either through ting and cache pollution.	epresented a security conce	rn when httpd participates in	any chain of proxies or	
CVE-2015-3197	https://nvd.nist.gov/vu In/detail/CVE-2015- 3197	2016-02-14	192.131.76.193	-	2018-05- 19T20:01:52.000Z
the-middle attackers to de	I.O.1 before 1.O.1r and 1.O.2 before tryptographic protection id get_client_hello functions.				
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	64.128.99.203	-	2018-05- 19T20:01:52.000Z
remote attackers to condu	ing implementation in the Apa uct HTTP request smuggling at naracters in modules/http/http_	tacks via a crafted request, r			
CVE-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	192.131.72.203	-	2018-05- 19T20:01:52.000Z
1.0.1m, and 1.0.2 before 1.0	ey function in s2_srvr.c in the S 0.2a accepts a nonzero CLIEN determine the MASTER-KEY v CVE-2016-0800.	Γ-MASTER-KEY CLEAR-KEY-I	ENGTH value for an arbitrary	cipher, which allows man-	
CVE-2015-3195	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	192.131.72.203	-	2018-05- 19T20:01:52.000Z
1.0.2 before 1.0.2e mishan	NE implementation in crypto/as Idles errors caused by malform memory by triggering a decod	ed X509_ATTRIBUTE data,	which allows remote attacker		
CVE-2016-0703	https://nvd.nist.gov/vu In/detail/CVE-2016- 0703	2016-03-02	64.128.99.203	-	2018-05- 19T20:01:52.000Z
1.0.1m, and 1.0.2 before 1.0	ey function in s2_srvr.c in the S 0.2a accepts a nonzero CLIEN [*] determine the MASTER-KEY v CVE-2016-0800.	Γ-MASTER-KEY CLEAR-KEY-I	ENGTH value for an arbitrary	cipher, which allows man-	
CVE-2015-3194	https://nvd.nist.gov/vu In/detail/CVE-2015- 3194	2015-12-06	64.128.99.203	-	2018-05- 19T20:01:52.000Z
	OpenSSL 1.0.1 before 1.0.1q an application crash) via an RSA P				
CVE-2016-8743	https://nvd.nist.gov/vu In/detail/CVE-2016- 8743	2017-07-27	208.11.141.92	-	2018-05- 19T20:01:52.000Z

19T20:01:52.000Z

19T20:01:52.000Z

П	29	~	ri	n	Hi.	\sim	n	٠

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3197 https://nvd.nist.gov/vu 2016-02-14 192.131.72.203 2018-05-

In/detail/CVE-2015-19T20:01:52.000Z

3197

Description:

ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-inthe-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.

https://nvd.nist.gov/vu 2018-05-CVE-2016-0703 2016-03-02 192.131.76.193

> In/detail/CVE-2016-19T20:01:52.000Z

0703

Description:

The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows manin-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

CVE-2015-3194 https://nvd.nist.gov/vu 2015-12-06 192.131.76.193 2018-05-

> In/detail/CVE-2015-19T20:01:52.000Z

3194

Description:

cryptorsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.

CVE-2014-0226 2018-05-

https://nvd.nist.gov/vu 2014-07-20 64.128.99.203

0226

In/detail/CVE-2014-

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3183 2015-07-20 208.11.141.92 https://nvd.nist.gov/vu 2018-05-

In/detail/CVE-2015-19T20:01:52.000Z

3183

Description:

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2015-3194 2018-05https://nvd.nist.gov/vu 2015-12-06 192.131.72.203

In/detail/CVE-2015-19T20:01:52.000Z

3194

Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.

CVE-2014-0226 2018-05https://nvd.nist.gov/vu 2014-07-20 208 11 141 92

> In/detail/CVE-2014-0226

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service

(heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3197 https://nvd.nist.gov/vu 2016-02-14 64.128.99.203 2018-05-

	In/detail/CVE-2015-				19T20:01:52.000Z		
	3197				13120.01.32.0002		
the-middle attackers to def	0.1 before 1.0.1r and 1.0.2 before tryptographic protection diget_client_hello functions.						
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	208.11.141.92	-	2018-05- 19T20:01:52.000Z		
directive may be associated	ed function in server/request. d with an authorization setting s in opportunistic circumstand	rather than an authentication	n setting, which allows remot	e attackers to bypass			
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	64.128.99.203	-	2018-05- 19T20:01:52.000Z		
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.							
CVE-2015-3195	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	192.131.76.193	-	2018-05- 19T20:01:52.000Z		
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.							
CVE-2015-3195	https://nvd.nist.gov/vu In/detail/CVE-2015- 3195	2015-12-06	64.128.99.203	-	2018-05- 19T20:01:52.000Z		
1.0.2 before 1.0.2e mishand	Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.						
CVE-2017-5647	https://nvd.nist.gov/vu In/detail/CVE-2017- 5647	2017-04-17	198.167.0.17	-	2018-05- 19T19:58:31.000Z		
Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.							
CVE-2017-5647	https://nvd.nist.gov/vu In/detail/CVE-2017- 5647	2017-04-17	198.167.0.48	-	2018-05- 19T19:58:31.000Z		
Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.							
CVE-2017-5647	https://nvd.nist.gov/vu In/detail/CVE-2017- 5647	2017-04-17	198.167.0.248		2018-05- 19T19:58:31.000Z		
and 6.0.0 to 6.0.52, when s	e pipelined requests in Apach send file was used, results in It in responses appearing to I	he pipelined request being lo	ost when send file processing	of the previous request			

C could see the correct response for request A, the response for request C for request B and no response for request C.

CVE-2017-5647 https://nvd.nist.gov/vu 2017-04-17 198.167.0.133 2018-05-

19T19:58:31.000Z In/detail/CVE-2017-

5647

Description:

A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.

CVE-2017-5647 https://nvd.nist.gov/vu 2017-04-17 198 167 0 33 2018-05-

In/detail/CVE-2017-

5647

19T19:58:31.000Z

A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.

CVE-2017-5647 https://nvd.nist.gov/vu 2017-04-17 192.131.72.236 2018-05-

In/detail/CVE-2017-

5647

Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and

C could see the correct response for request A, the response for request C for request B and no response for request C.

https://nvd.nist.gov/vu CVE-2017-5647 2017-04-17 198.167.0.148 2018-05-

In/detail/CVE-2017-

5647

19T19:58:31.000Z

Description:

A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.

https://nvd.nist.gov/vu CVE-2017-5647 2017-04-17 198 167 0 246 2018-05-

In/detail/CVE-2017-

5647

19T19:58:31.000Z

19T19:58:31.000Z

Description:

A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.64 2018-05-

In/detail/CVE-2014-

0226

19T12:44:21.000Z

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.76 2018-05-In/detail/CVE-2014-

0226

19T12:44:21.000Z

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 208.11.141.76 - 2018-05-

In/detail/CVE-2017-

3737

19T12:44:21.000Z

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.11.141.204 - 2018-05-

In/detail/CVE-2017-

3736

19T12:44:21.000Z

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.76 - 2018-05-

In/detail/CVE-2016-

8743

19T12:44:21.000Z

Description

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 208.11.141.177 - 2018-05-

In/detail/CVE-2017-

3737

19T12:44:21.000Z

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.132 - 2018-05-

In/detail/CVE-2016-

8743

19T12:44:21.000Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.78 - 2018-05-

In/detail/CVE-2015-

3185

200.11.141.76 - 2010-03

19T12:44:21.000Z

19T12:44:21.000Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.88 - 2018-05-

In/detail/CVE-2014-

0226

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.11.141.192 2018-05-

In/detail/CVE-2015-19T12:44:21.000Z

3183

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.167 2018-05-

> In/detail/CVE-2015-19T12:44:21.000Z

3185

Description:

The an_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

208.11.141.75 CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 2018-05-

In/detail/CVE-2014-19T12:44:21.000Z

0226

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.11.141.196 2018-05-

> In/detail/CVE-2015-19T12:44:21.000Z

3183

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.192 2018-05-

> In/detail/CVE-2016-19T12:44:21.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

2018-05-CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.11.141.132

In/detail/CVE-2015-

3183

19T12:44:21.000Z

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2017-3738 https://nvd.nist.gov/vu 208.11.141.177 2018-05-2017-12-07 In/detail/CVE-2017-19T12:44:21.000Z

3738

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-

19T12:44:21.000Z

19T12:44:21.000Z

2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation), Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.11.141.91 2018-05-

In/detail/CVE-2017-

3738

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.177 2018-05-

In/detail/CVE-2014-

0226

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.91 2018-05-

In/detail/CVE-2014-

0226

19T12:44:21.000Z

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2014-0226 2014-07-20 2018-05https://nvd.nist.gov/vu 208.11.141.196

In/detail/CVE-2014-

0226

19T12:44:21.000Z

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.155 2018-05-

In/detail/CVE-2015-

3185

19T12:44:21.000Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.177 2018-05-

In/detail/CVE-2015-

3185

19T12:44:21.000Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2015-3185 208.11.141.132 https://nvd.nist.gov/vu 2015-07-20 2018-05-19T12:44:21.000Z

In/detail/CVE-2015-

3185

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.11.141.92 2018-05-

> In/detail/CVE-2017-19T12:44:21.000Z

3736

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.11.141.204 2018-05-

In/detail/CVE-2015-

3183

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.11.141.177 2018-05-

In/detail/CVE-2015-

3183

19T12:44:21.000Z

19T12:44:21.000Z

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.177 2018-05-

In/detail/CVE-2016-

8743

19T12:44:21.000Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVF-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.11.141.204 2018-05-

In/detail/CVE-2017-

3738

19T12:44:21.000Z

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.91 2018-05-

In/detail/CVE-2016-

19T12:44:21.000Z

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.155 2018-05-

In/detail/CVE-2016-

8743

19T12:44:21.000Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.11.141.75 2018-05-

In/detail/CVE-2015-19T12:44:21.000Z

3183

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

2018-05-CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.75

> In/detail/CVE-2015-19T12:44:21.000Z

3185

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

https://nvd.nist.gov/vu CVE-2015-3183 208.11.141.155 2018-05-2015-07-20

> In/detail/CVE-2015-19T12:44:21.000Z

3183

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.204 2018-05-

> In/detail/CVE-2016-19T12:44:21.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.196 2018-05-

> In/detail/CVE-2016-19T12:44:21.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.11.141.76 2018-05-

> In/detail/CVE-2015-19T12:44:21.000Z

3183

3185

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

208.11.141.192 CVE-2015-3185 https://nvd.nist.gov/vu 2018-05-2015-07-20 19T12:44:21.000Z

In/detail/CVE-2015-

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVF-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208 11 141 73 2018-05-

In/detail/CVE-2016-

19T12:44:21.000Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2016-8743 2017-07-27 https://nvd.nist.gov/vu 208.11.141.75 2018-05-

In/detail/CVE-2016-

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 208.11.141.204 2018-05-

In/detail/CVE-2017-

3737

19T12:44:21.000Z

19T12:44:21.000Z

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2017-3736 https://nvd.nist.gov/vu 2017-11-02 208.11.141.177 2018-05-

In/detail/CVE-2017-

3736

19T12:44:21.000Z

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.78 2018-05-In/detail/CVE-2016-

8743

19T12:44:21.000Z

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2017-3737 https://nvd.nist.gov/vu 2017-12-07 208.11.141.92 2018-05-

In/detail/CVE-2017-

3737

19T12:44:21.000Z

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.64 2018-05-

In/detail/CVE-2016-

19T12:44:21.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

2014-07-20

CVE-2014-0226

https://nvd.nist.gov/vu

208.11.141.78

2018-05-

In/detail/CVE-2014-

0226

19T12:44:21.000Z

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3737

https://nvd.nist.gov/vu 2017-12-07

208.11.141.91

2018-05-

In/detail/CVE-2017-

3737

19T12:44:21.000Z

Description:

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2017-3736

https://nvd.nist.gov/vu 2017-11-02

208.11.141.76

2018-05-

In/detail/CVE-2017-

3736

19T12:44:21.000Z

Description:

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BM1, BM12 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2015-3183

https://nvd.nist.gov/vu In/detail/CVE-20152015-07-20

208.11.141.167

2018-05-

19T12:44:21.000Z

3183

Description:

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2014-0226

https://nvd.nist.gov/vu In/detail/CVE-20142014-07-20

208.11.141.73

2018-05-

19T12:44:21.000Z

0226

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3738

https://nvd.nist.gov/vu ln/detail/CVE-2017-

3738

2017-12-07

208.11.141.92

2018-05-

19T12:44:21.000Z

Description

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on

TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2016-8743 https://nvd.nist.gov/vu 2017-07-27 208.11.141.88 - 2018-05-

In/detail/CVE-2016- 19T12:44:21.000Z

8743

Description:

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.88 - 2018-05-

In/detail/CVE-2015- 19T12:44:21.000Z

3185

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2017-3738 https://nvd.nist.gov/vu 2017-12-07 208.11.141.76 - 2018-05-

In/detail/CVE-2017- 19T12:44:21.000Z

3738

Description:

There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.204 - 2018-05-

In/detail/CVE-2014- 19T12:44:21.000Z

0226

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3183 https://nvd.nist.gov/vu 2015-07-20 208.11.141.88 - 2018-05-

In/detail/CVE-2015- 19T12:44:21.000Z

3183

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/filters.c.

CVE-2015-3185 https://nvd.nist.gov/vu 2015-07-20 208.11.141.91 - 2018-05-

In/detail/CVE-2015- 19T12:44:21.000Z

3185

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.1d does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2014-0226 https://nvd.nist.gov/vu 2014-07-20 208.11.141.132 - 2018-05-

In/detail/CVE-2014- 19T12:44:21.000Z

0226

Description:

Description:

(heap-based buffer overflo	d_status module in the Apache ow), or possibly obtain sensitiv dling within the status_handler ia_request.c.	e credential information or ex	xecute arbitrary code, via a cr	afted request that triggers	
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	208.11.141.167	-	2018-05- 19T12:44:21.000Z
(heap-based buffer overflo	d_status module in the Apache ow), or possibly obtain sensitiv dling within the status_handler a_request.c.	e credential information or ex	xecute arbitrary code, via a cr	afted request that triggers	
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	208.11.141.196	-	2018-05- 19T12:44:21.000Z
directive may be associate	ired function in server/request. ed with an authorization setting ins in opportunistic circumstand	g rather than an authenticatio	on setting, which allows remot	te attackers to bypass	
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	208.11.141.76	-	2018-05- 19T12:44:21.000Z
directive may be associate	ired function in server/request. ed with an authorization setting ins in opportunistic circumstand	g rather than an authenticatio	on setting, which allows remot	te attackers to bypass	
CVE-2015-3185	https://nvd.nist.gov/vu In/detail/CVE-2015- 3185	2015-07-20	208.11.141.73	-	2018-05- 19T12:44:21.000Z
directive may be associate	ired function in server/request. ed with an authorization setting ns in opportunistic circumstand	g rather than an authenticatio	on setting, which allows remot	te attackers to bypass	
CVE-2014-0226	https://nvd.nist.gov/vu In/detail/CVE-2014- 0226	2014-07-20	208.11.141.155	-	2018-05- 19T12:44:21.000Z
(heap-based buffer overflo	d_status module in the Apache ow), or possibly obtain sensitiv dling within the status_handler a_request.c.	e credential information or ex	xecute arbitrary code, via a cr	afted request that triggers	
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	208.11.141.64	-	2018-05- 19T12:44:21.000Z
remote attackers to condu	ling implementation in the Apa uct HTTP request smuggling at haracters in modules/http/http.	tacks via a crafted request, r			
CVE-2015-3183	https://nvd.nist.gov/vu In/detail/CVE-2015- 3183	2015-07-20	208.11.141.78	-	2018-05- 19T12:44:21.000Z
remote attackers to condu	ling implementation in the Apa uct HTTP request smuggling at haracters in modules/http/http_	tacks via a crafted request, r			

208.11.141.192

2018-05-

19T12:44:21.000Z

CVE-2014-0226

https://nvd.nist.gov/vu

In/detail/CVE-2014-

2014-07-20

0226

3185

Description:

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3185

https://nvd.nist.gov/vu In/detail/CVE-2015-

vu 2015-07-20

208.11.141.204

2018-05-

19T12:44:21.000Z

Description:

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

RECOMMENDATION

Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the BugTraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.

ABOUT THIS ISSUE

Based on scan data, the company had medium severity CVE vulnerability that was open longer than 60 days after the CVE was published. Medium severity CVEs are those with a documented CVSS severity between 4.0 and 6.9. It is best practice to mitigate or patch medium severity vulnerabilities within 60 days. Details on each vulnerability are listed in the table below.

22



ENDPOINT SECURITY

ISSUE COUNT

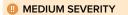
The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

The Endpoint Security Module tracks identification points that are extracted from metadata related to the operating system, web browser, and related active plugins. The information gathered allows companies to identify outdated versions of these data points which can lead to client-side exploitation attacks.

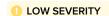


There are no High Risk Issues to



Outdated Web Browser

Outdated Operating System



There are no Low Risk Issues to



There are no Positive Risk Issues to



Multiple Browsers Detected

ENDPOINT SECURITY > ISSUE DETAIL

Outdated Web Browser Observed

An outdated web browser connected to a web server.

-0.4 SCORE **IMPACT**

22 findings

SOURCE IP	PRODUCT MANUFACTURER	PRODUCT NAME	PRODUCT TYPE	PRODUCT VERSION	PRODUCT LATEST VERSION	LAST SEEN
12.180.126.100	Google	Chrome	browser	61.0.3163.79	69.0.3497.100	2019-01- 31T02:00:00.000Z
208.66.22.2	Google	Chrome	browser	65.0.3325.162	69.0.3497.100	2019-01- 30T23:00:00.000 Z
204.95.150.205	Google	Chrome	browser	65.0.3325.181	69.0.3497.100	2019-01- 30T20:08:39.000 Z
65.202.81.138	Google	Chrome	browser	66.0.3359.139	69.0.3497.100	2019-01- 30T17:15:50.000Z
204.95.150.205	Microsoft	Edge	browser	14.14393	42.17134.1.0	2019-01- 30T16:57:45.000Z
103.1.128.11	Google	Chrome	browser	44.0.2403.89	69.0.3497.100	2019-01- 30T07:38:29.000 Z
12.27.169.18	Apple	Safari	browser	9.1.2	12.0	2019-01- 29T20:33:50.000 Z

12.16.164.205	Microsoft	Edge	browser	14.14393	42.17134.1.0	2019-01- 29T15:42:21.000Z
208.66.22.2	Microsoft	Edge	browser	14.14393	42.17134.1.0	2019-01- 29T14:32:30.000Z
103.1.128.11	Google	Chrome	browser	51.0.2704.84	69.0.3497.100	2019-01- 29T08:23:15.000Z
166.73.28.27	Google	Chrome	browser	42.0.2311.152	69.0.3497.100	2019-01- 28T20:34:50.000 Z
166.73.228.150	Google	Chrome	browser	43.0.2357.130	69.0.3497.100	2019-01- 28T18:33:26.000Z
103.1.128.11	Google	Chrome	browser	33.0.1736.2	69.0.3497.100	2019-01- 28T10:54:48.000Z
12.180.126.100	Google	Chrome	browser	64.0.3282.119	69.0.3497.100	2019-01- 27T22:57:46.000Z
12.175.11.5	Microsoft	Edge	browser	14.14393	42.17134.1.0	2019-01- 25T18:25:37.000Z
12.2.10.242	Google	Chrome	browser	65.0.3325.162	69.0.3497.100	2019-01- 22T16:33:05.000Z
12.2.10.242	Microsoft	Edge	browser	14.14393	42.17134.1.0	2019-01- 22T16:15:19.000Z
103.1.131.254	Google	Chrome	browser	62.0.3202.94	69.0.3497.100	2019-01- 11T14:00:00.000Z
64.149.173.195	Mozilla	Firefox	browser	56.0	62.0.2	2019-01- 09T17:18:17.000Z
208.66.22.2	Mozilla	Firefox	browser	56.0	62.0.2	2019-01- 06T12:59:18.000Z
65.206.30.70	Apple	Safari	browser	9.1.1	12.0	2019-01- 03T14:00:48.000Z
166.73.129.157	Google	Chrome	browser	60.0.3112.113	69.0.3497.100	2019-01- 02T21:49:19.000Z

RECOMMENDATION

Update the web browsers in question. Enable automatic updates if available from your web browser vendor and permitted in your environment.

ABOUT THIS ISSUE

The web is constantly evolving, using different languages, protocols, and file formats over time. Web browsers regularly release new versions, on time scales as short as every six weeks. These new versions frequently contain security and stability fixes. When a web browser connects to a web server, it informs the server its platform and version information. This information assists the server in providing appropriate content. The information can also be recorded and aggregated to determine what platforms and browser versions are being used by hosts at various places on the Internet. Using such a data set, it was found that an outdated web browser was in use as described in the table below. Note that a single external IP address, such as those in the table below, may correspond to any number of internal hosts. For example, a company firewall or NAT gateway with a single external IP will appear to be the source of an entire network full of corporate desktops.



ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

The IP Reputation and Malware Exposure module makes use of the SecurityScorecard sinkhole infrastructure as well as a blend of OSINT malware feeds, and third party threat intelligence data sharing partnerships. The SecurityScorecard sinkhole system ingests millions of malware signals from commandeered Command and Control (C2) infrastructures globally from all over the world. The incoming data is processed and attributed to corporate enterprises. The quantity and duration of malware infections are used as the determining factor for calculating is module the Malware Exposure Key Threat Indicator.



IP REPUTATION > ISSUE DETAIL

Malware Events, Last Year

Communications indicative of malware infections were observed over the last 365 days.

2 findings

MALWARE TYPE	MALWARE FAMILY	MALWARE DETECTION METHODS	SOURCE IP	FIRST SEEN	LAST SEEN
bot	azorult	honeynet	103.1.130.48	2018-06- 06T00:00:00.000Z	2018-06- 06T00:00:00.000Z
bot	quant	honeynet	12.179.188.5	2018-03- 26T00:00:00.000Z	2018-03- 27T00:00:00.000Z

RECOMMENDATION

Investigate the devices associated with the IP addresses listed, checking for evidence of malware infections.

ABOUT THIS ISSUE

After a device has been infected by malware, it often communicates with a command and control (C&C) service on the internet. This service allows the malware to register its infected device and receive instructions from the malware's authors. These instructions could cause the device to delete or encrypt its datastores, participate in distributed denial-of-service (DDoS) attacks, or perform any variety of malicious actions.



58 APPLICATION SECURITY

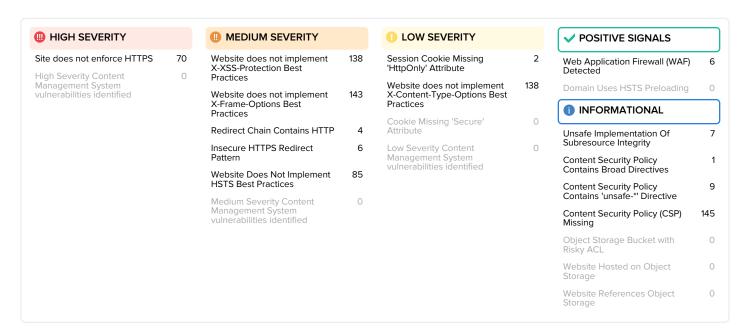
ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

The Web Application Vulnerability module uses incoming threat intelligence from known exploitable conditions identified via: whitehat CVE databases, blackhat exploit databases, and sensitive findings indexed by major search engines. The module ingests data from multiple public data sets, third party feeds, and an internal proprietary indexing and aggregation engine.

The score determines the likelihood of an upcoming web application breach, and checks for any existing defacement code. Presence of vulnerable applications, outdated versions, and active defacements are used to calculate the overall grade.



APPLICATION SECURITY > ISSUE DETAIL

Website does not implement X-XSS-Protection Best Practices

Not explicitly setting X-XSS-Protection means that clients viewing a website could be at risk of reflected Cross-site Scripting (XSS) attacks.

-0.9 SCORE

138 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
x_xss_protection_mis sing	https://staging.fiserv- ecomhosting.com/	https://staging.fiserv- ecomhosting.com/	n/a	Header missing	2019-01- 29T09:11:43.731Z
x_xss_protection_mis sing	http://staging.fiserv- ecomhosting.com/	http://staging.fiserv- ecomhosting.com/	n/a	Header missing	2019-01- 29T09:11:43.673Z
x_xss_protection_mis sing	http://www.fiservsw.c om/	http://www.fiservsw.co m/	n/a	Header missing	2019-01- 29T09:11:42.823Z

x_xss_protection_mis sing	https://mail.fiservlendi ngsolutions.com/	https://mail.fiservlendi ngsolutions.com/	n/a	Header missing	2019-01- 29T09:11:17.099Z
x_xss_protection_mis sing	http://fiservcreditservices.com/	http://fiservcreditservices.com/	n/a	Header missing	2019-01- 29T09:11:15.569Z
x_xss_protection_mis sing	https://webmail.fiserv. net/	https://webmail.fiserv. net/	n/a	Header missing	2019-01- 29T09:11:13.849Z
x_xss_protection_mis sing	http://fiservsw.com/	http://fiservsw.com/	n/a	Header missing	2019-01- 29T09:11:05.384Z
x_xss_protection_mis sing	https://fiserv.service-now.com/auth_redire ct.do? sysparm_url=https%3 a%2f%2flogin.microso ftonline.com%2fte%2ff iservservicepoint.onm icrosoft.com%2fb2c_1 a_prod_sn_signin%2f samlp%2fsso%2flogin %3fsamlrequest%3dlvl bbptaep0vthdgoxfjvs yssvxvupki2o2hf2sdg 7mszjcdhsr%252fx8a kts%252bwep15896b n7ni3drxq7lopeedphf aznttamr17qsis6his2gf ugfwrld77o5wxyfursv hbdxcy5jboko4iesuab sh25scfj7cpuljuzzvgfz mapubn1s%252b0ktq uboi7lt9gqak4w0haw b1ypr3rqatwaaxhswm yhhwbmeadtctzpwtgx qb4qd2qt3em2ouhxnl 5zhxyoaebsnxwtzkpjo %252f8l6rlwbkihwvrh met9umyn%252bw25 2fwzz6uutfnxyvchlhe qrf4ssyizfy%252buqx quqa5fwzmx5s4ww3tj j3sen2gl0qyhklvoz8o dnirewrkjk4sulfwsvnc g8mlgzpl%252fn%25 2bpinyft8ccj%25zf%252fst9mbl0pwd4p6p %252bk%252bhdynm iemmv6nd1btbbt5xe4 7ei%252f312sl0uvws8 cs1yrrte7bu61kd68rk7 pzwnbu48yh5s02l32 mfzm6vctvlxjwuwanqj xs%252bq%252ff3d7%252baw%253d%253d %26relaystate%3dhttp s%253a%252fr%252ffi serv.service-now.com%252fnavpa ge.do	http://my.carreker.com /	http://my.carreker.com /, 302, https://c3.fiserv.com/, 302, https://servicepoint.fis ervapps.com/, 302, https://fiserv.service-now.com/, 302, https://fiserv.service-now.com/, 302, https://fiserv.service-now.com/, 302, https://fiserv.service-now.com/auth_redirect.do? sysparm_url=https%3 A%2F%2Flogin.microsoftonline.com%2Fte% 2Ffiservservicepoint.onmicrosoft.com%2F82 C_1A_Prod_sn_signin%2Fsamlp%2Fsso%2Flogin%3FSAMLRequest%3DIVLBbptAEPOVtHdgoXFjVsySsVXVUpKi2O2hF2sDg7MSzJCdhSR%252FX8AkTS%252BWep15896bN7Ni3dRxq7LOPeEDPHfAznttamR17qSis6hls2GFugFWrlD77O5WxYFUrSVHBdXCy5jBOkO4leSuAbsH25sCfj7cpuLJuzZVGFZmAPUBn1s%252B0ktQUBOi7lt9gqAk4W0HAwb1yPR3rqaTwaAxhSWmyhHWBmEadTCTzpwtGXQB4Qd2Qt3Em2OUHXNL5ZHxyOaEBsNxwTZkpjO%252F8L6RLWBKlhWVrhmEt9umYn%252B%252FWZZ6UUTFNXyVchlHEqrF4ssyiZfy%252BuqxquQA5Fwzmx5S4Ww3TjJ3sEN2Gl0qYhklvoz8ODnlREWRjK4SuLfwsvnCG8MlgZPl%252FN%252BPlNYfT8ccj%252F%252FsT9MBL0pwd4P6P%252BK%252BhdynmlemMV6Nd1bTbbt5xe47Ei%252F312sL0uvws8Cs1yrRte7bU61Kd68rK7pZWNBu48Yh5s02l32MFZM6VcTVLXjWuwAnQjXs%252Bq%25	Header missing	2019-01- 29T09:11:00.692Z

			2FD77%252BAw%253 D%253D%26RelaySta te%3Dhttps%253A%2 52F%252Ffiserv.servi ce- now.com%252Fnavpa ge.do		
x_xss_protection_mis sing	https://search.carreke r.com/	https://search.carreker .com/	n/a	Header missing	2019-01- 29T09:10:57.094Z
x_xss_protection_mis sing	http://search.carreker. com/	http://search.carreker. com/	n/a	Header missing	2019-01- 29T09:10:57.065Z
x_xss_protection_mis sing	https://careers.carrek er.com/	https://careers.carreke r.com/	n/a	Header missing	2019-01- 29T09:10:56.934Z
x_xss_protection_mis sing	https://mail.billmatrix.c om/	https://mail.billmatrix.c om/	n/a	Header missing	2019-01- 29T09:10:56.928Z
x_xss_protection_mis sing	http://careers.carreker .com/	http://careers.carreker .com/	n/a	Header missing	2019-01- 29T09:10:56.855Z
x_xss_protection_mis sing	https://support.fiservat lanta.net/	http://support.fiservatl anta.net/	http://support.fiservatl anta.net/, 302, https://support.fiservat lanta.net/	Header missing	2019-01- 29T09:10:54.014Z
x_xss_protection_mis sing	https://fiservwebsoluti ons.com/	https://fiservwebsoluti ons.com/	n/a	Header missing	2019-01- 29T09:10:53.876Z
x_xss_protection_mis sing	https://alpha.hepsiian. com/	https://alpha.hepsiian. com/	n/a	Header missing	2019-01- 29T09:10:53.348Z
x_xss_protection_mis sing	https://images.hepsiia n.com/	https://images.hepsiia n.com/	n/a	Header missing	2019-01- 29T09:10:52.534Z
x_xss_protection_mis sing	https://fiservlendingso lutions.com/	https://fiservlendingsol utions.com/	n/a	Header missing	2019-01- 29T09:10:50.983Z
x_xss_protection_mis sing	http://fiservlendingsol utions.com/	http://fiservlendingsol utions.com/	n/a	Header missing	2019-01- 29T09:10:50.913Z
x_xss_protection_mis sing	https://fiservipvpn.co m/	https://fiservipvpn.com /	n/a	Header missing	2019-01- 29T09:10:50.584Z
x_xss_protection_mis sing	http://demo.billmatrix. com/	http://demo.billmatrix. com/	n/a	Header missing	2019-01- 29T09:10:50.447Z
x_xss_protection_mis sing	https://www.fiservlend ingsolutions.com/	https://www.fiservlend ingsolutions.com/	n/a	Header missing	2019-01- 29T09:10:50.369Z
x_xss_protection_mis sing	http://mail.fiservlendin gsolutions.com/	http://mail.fiservlendin gsolutions.com/	n/a	Header missing	2019-01- 29T09:10:50.349Z
x_xss_protection_mis sing	http://www.fiservlendi ngsolutions.com/	http://www.fiservlendi ngsolutions.com/	n/a	Header missing	2019-01- 29T09:10:50.285Z
x_xss_protection_mis sing	https://fiservcws.com/	https://fiservcws.com/	n/a	Header missing	2019-01- 29T09:10:50.069Z
x_xss_protection_mis sing	https://www.careers.fi serv.com/	https://careers.fiserv.c om/	https://careers.fiserv.c om/, 301, http://www.careers.fis erv.com, 301,	Header missing	2019-01- 29T09:09:27.681Z

			https://www.careers.fi serv.com/		
x_xss_protection_mis sing	https://alabama.fiservl s.com/	https://alabama.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:16.824Z
x_xss_protection_mis sing	http://alabama.fiservls. com/	http://alabama.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:16.763Z
x_xss_protection_mis sing	https://en.fiservls.com /	https://en.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:16.760Z
x_xss_protection_mis sing	https://blog.fiservls.co m/	https://blog.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:16.759Z
x_xss_protection_mis sing	https://ca.fiservls.com/	https://ca.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:16.742Z
x_xss_protection_mis sing	https://shop.fiservls.co m/	https://shop.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:16.731Z
x_xss_protection_mis sing	https://bg.fiservls.com /	https://bg.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:16.726Z
x_xss_protection_mis sing	https://bf.fiservls.com/	https://bf.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:16.715Z
x_xss_protection_mis sing	http://ca.fiservls.com/	http://ca.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:16.691Z
x_xss_protection_mis sing	http://en.fiservls.com/	http://en.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:16.691Z
x_xss_protection_mis sing	http://blog.fiservls.co m/	http://blog.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:16.677Z
x_xss_protection_mis sing	http://shop.fiservls.co m/	http://shop.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:16.662Z
x_xss_protection_mis sing	http://bg.fiservls.com/	http://bg.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:16.662Z
x_xss_protection_mis sing	http://bf.fiservls.com/	http://bf.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:16.646Z
x_xss_protection_mis sing	https://ap.fiservls.com/	https://ap.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.968Z
x_xss_protection_mis sing	https://in.fiservls.com/	https://in.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.961Z
x_xss_protection_mis sing	https://ww.fiservls.co m/	https://ww.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:14.955Z
x_xss_protection_mis sing	https://backend.fiservl s.com/	https://backend.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:14.953Z
x_xss_protection_mis sing	https://espanol.fiservls .com/	https://espanol.fiservls .com/	n/a	Header missing	2019-01- 22T07:04:14.953Z
x_xss_protection_mis sing	https://chat.fiservls.co m/	https://chat.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:14.953Z
x_xss_protection_mis sing	https://arizona.fiservls. com/	https://arizona.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:14.918Z

x_xss_protection_mis sing	http://ns1.fiservls.com/	http://ns1.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.897Z
x_xss_protection_mis sing	http://ww.fiservls.com/	http://ww.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.897Z
x_xss_protection_mis sing	http://download.fiservl s.com/	http://download.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:14.897Z
x_xss_protection_mis sing	http://ap.fiservls.com/	http://ap.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.897Z
x_xss_protection_mis sing	http://backend.fiservls .com/	http://backend.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:14.878Z
x_xss_protection_mis sing	http://in.fiservls.com/	http://in.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.878Z
x_xss_protection_mis sing	http://espanol.fiservls. com/	http://espanol.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:14.863Z
x_xss_protection_mis sing	http://forums.fiservls.c om/	http://forums.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:14.853Z
x_xss_protection_mis sing	http://arizona.fiservls.c om/	http://arizona.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:14.849Z
x_xss_protection_mis sing	http://chat.fiservls.co m/	http://chat.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:14.849Z
x_xss_protection_mis sing	https://14.fiservls.com/	https://14.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.091Z
x_xss_protection_mis sing	https://mobile.fiservls.com/	https://mobile.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.089Z
x_xss_protection_mis sing	https://sadmin.fiservls. com/	https://sadmin.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:14.085Z
x_xss_protection_mis sing	https://boston.fiservls.com/	https://boston.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.083Z
x_xss_protection_mis sing	https://developer.fiser vls.com/	https://developer.fiser vls.com/	n/a	Header missing	2019-01- 22T07:04:14.073Z
x_xss_protection_mis sing	https://act.fiservls.com /	https://act.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:14.070Z
x_xss_protection_mis sing	https://arlington.fiservl s.com/	https://arlington.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:14.063Z
x_xss_protection_mis sing	https://client.fiservls.c om/	https://client.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:14.063Z
x_xss_protection_mis sing	https://ftp.fiservls.com /	https://ftp.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.047Z
x_xss_protection_mis sing	http://mobile.fiservls.c om/	http://mobile.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:14.017Z
x_xss_protection_mis sing	http://14.fiservls.com/	http://14.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.016Z
x_xss_protection_mis	http://boston.fiservls.c	http://boston.fiservls.c	n/a	Header missing	2019-01-

sing	om/	om/			22T07:04:14.015Z
x_xss_protection_mis sing	http://sadmin.fiservls.c om/	http://sadmin.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:14.014Z
x_xss_protection_mis sing	http://developer.fiserv ls.com/	http://developer.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:13.993Z
x_xss_protection_mis sing	http://act.fiservls.com/	http://act.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:13.993Z
x_xss_protection_mis sing	http://client.fiservls.co m/	http://client.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:13.990Z
x_xss_protection_mis sing	http://backup.fiservls.c om/	http://backup.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:13.984Z
x_xss_protection_mis sing	http://ftp.fiservls.com/	http://ftp.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:13.780Z
x_xss_protection_mis sing	https://blackberry.fiser vls.com/	https://blackberry.fiser vls.com/	n/a	Header missing	2019-01- 22T07:04:13.296Z
x_xss_protection_mis sing	https://citrix.fiservls.co m/	https://citrix.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:13.214Z
x_xss_protection_mis sing	https://arkansas.fiservl s.com/	https://arkansas.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:13.209Z
x_xss_protection_mis sing	https://biz.fiservls.com /	https://biz.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:13.207Z
x_xss_protection_mis sing	http://citrix.fiservls.co m/	http://citrix.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:13.145Z
x_xss_protection_mis sing	http://blackberry.fiserv ls.com/	http://blackberry.fiserv ls.com/	n/a	Header missing	2019-01- 22T07:04:13.145Z
x_xss_protection_mis sing	http://arkansas.fiservls .com/	http://arkansas.fiservls .com/	n/a	Header missing	2019-01- 22T07:04:13.145Z
x_xss_protection_mis sing	http://biz.fiservls.com/	http://biz.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:13.145Z
x_xss_protection_mis sing	https://survey.fiservls. com/	https://survey.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:12.891Z
x_xss_protection_mis sing	https://demo.fiservls.c om/	https://demo.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:12.891Z
x_xss_protection_mis sing	https://au.fiservls.com/	https://au.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:12.849Z
x_xss_protection_mis sing	http://survey.fiservls.c om/	http://survey.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:12.815Z
x_xss_protection_mis sing	http://demo.fiservls.co m/	http://demo.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:12.815Z
x_xss_protection_mis sing	http://arlington.fiservls .com/	http://arlington.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:05.405Z
x_xss_protection_mis sing	https://fiservsupport.c om/	http://www.fiservsupp ort.com/	http://www.fiservsupp ort.com/, 302,	Header missing	2019-01- 22T07:04:04.073Z

				http://fiservsupport.co		
				m/, 302, https://fiservsupport.c		
Sing	x_xss_protection_mis sing	http://fiservdox.com/	http://fiservdox.com/	n/a	Header missing	
	x_xss_protection_mis sing	•	•	n/a	Header missing	
	x_xss_protection_mis sing	https://ac.fiservls.com/	https://ac.fiservls.com/	n/a	Header missing	
sing m/ m/ m/ m/ 22T07-04-03 0132 x_xss_protection_mis sing // // // // // // // // // // // // //	x_xss_protection_mis sing	http://mail.fiservls.com /	http://mail.fiservls.com /	n/a	Header missing	
	x_xss_protection_mis sing	•	•	n/a	Header missing	
	x_xss_protection_mis sing	https://ns1.fiservls.com /	https://ns1.fiservls.com /	n/a	Header missing	
22T07:04:02.968Z	x_xss_protection_mis sing	https://131.fiservls.com /	https://131.fiservls.com /	n/a	Header missing	
sing com/ com/ com/ com/ com/ com/ com/ com/	x_xss_protection_mis sing	http://ac.fiservls.com/	http://ac.fiservls.com/	n/a	Header missing	
sing // / / / / / / / / / / / / / / / / /	x_xss_protection_mis sing	•	· ·	n/a	Header missing	
sing m/ m/ 22T07:04:02.904Z x_xss_protection_mis sing http://131.fiservls.com/ http://131.fiservls.com/ n/a Header missing 2019-01-22T07:04:02.897Z x_xss_protection_mis sing https://apps.fiservls.co https://apps.fiservls.co n/a Header missing 2019-01-22T07:04:02.857Z x_xss_protection_mis sing https://atlanta.fiservls.com/ n/a Header missing 2019-01-22T07:04:02.851Z x_xss_protection_mis sing http://corp.fiservls.com/ n/a Header missing 2019-01-22T07:04:02.819Z x_xss_protection_mis sing http://apps.fiservls.com/ n/a Header missing 2019-01-22T07:04:02.819Z x_xss_protection_mis sing https://apps.fiservls.com/ n/a Header missing 2019-01-22T07:04:02.789Z x_xss_protection_mis sing https://customer.fiservls.com/ n/a Header missing 2019-01-22T07:04:02.784Z x_xss_protection_mis sing https://intranet1.fiservls.com/ https://intranet1.fiservls.com/ n/a Header missing 2019-01-22T07:04:02.756Z x_xss_protection_mis http://atlanta.fiservls.com/ http://atlanta.fiservls.com/ n/a Header mis	x_xss_protection_mis sing		http://pop.fiservls.com /	n/a	Header missing	
sing 22T07:04:02.897Z x_xss_protection_mis https://apps.fiservls.co m/ https://apps.fiservls.co m/ https://apps.fiservls.co m/ https://atlanta.fiservls. n/a Header missing 2019-01- 22T07:04:02.857Z x_xss_protection_mis https://corp.fiservls.co m/ https://corp.fiservls.com n/a Header missing 2019-01- 22T07:04:02.851Z x_xss_protection_mis http://corp.fiservls.co m/ http://corp.fiservls.co m/ http://apps.fiservls.co m/ http://apps.fiservls.co m/ https://customer.fiserv ls.co m/ https://customer.fiserv ls.com/ s.com/ s.com/ https://customer.fiserv ls.com/ s.com/ https://intranet1.fiservl s.com/ https://intranet1.fiservl s.com/ https://intranet1.fiservl s.com/ https://allanta.fiservls.co m/ https://allanta.fiservls.com/ https://allanta.fiservls.com/ https://allanta.fiservls.com/ https://allanta.fiservls.com/ https://allanta.fiservls.com/ https://allanta.fiservls.com/ n/a Header missing 2019-01- 22T07:04:02.748Z x_xss_protection_mis https://allanta.fiservls.com/ https://allanta.fiservls.com/ n/a Header missing 2019-01- 22T07:04:02.748Z	x_xss_protection_mis sing		·	n/a	Header missing	
sing m/ m/ style="color: blue;"/atlanta.fiservls." blue;//atlanta.fiservls. com/ blue;//atlanta.fiservls. com/ blue;//atlanta.fiservls. com/ blue;//atlanta.fiservls. com/ blue;//atlanta.fiservls. com/ blue;//atlanta.fiservls. com/ blue;//apps.fiservls.com n/a http://apps.fiservls.co m/ blue;//apps.fiservls.com n/a http://apps.fiservls.co m/ blue;//apps.fiservls.co m/ blue;//allanta.fiservl s.com/ blue;//allanta.fiservl s.com/ blue;//allanta.fiservls.com/ blue;//atlanta.fiservls.com/ blue;//atlan	x_xss_protection_mis sing	http://131.fiservls.com/	http://131.fiservls.com/	n/a	Header missing	
sing com/ com/ com/ 22T07:04:02.851Z x_xss_protection_mis sing http://corp.fiservls.co m/ / http://corp.fiservls.com n/a Header missing 2019-01- 22T07:04:02.819Z x_xss_protection_mis http://apps.fiservls.co m/ / https://customer.fiservls.co m/ / https://customer.fiservls.co m/ / s.com/ s.com/ s.com/ https://customer.fiservls.co m/ / https://customer.fiservls.co m/ / https://customer.fiservls.co m/ / https://customer.fiservls.com/ s.com/ s.com/ https://intranet1.fiservls.com/ s.com/ https://intranet1.fiservls.com/ s.com/ https://intranet1.fiservls.com/ https://intranet1.fiservls.com/ n/a Header missing 2019-01- 22T07:04:02.756Z x_xss_protection_mis http://atlanta.fiservls.c om/ https://latlanta.fiservls.c om/ / https://latlanta.fiservls.com/ n/a Header missing 2019-01- 22T07:04:02.748Z	x_xss_protection_mis sing			n/a	Header missing	
sing m/ / 22T07:04:02.819Z x_xss_protection_mis http://apps.fiservls.co m/ n/a Header missing 2019-01- 22T07:04:02.789Z x_xss_protection_mis https://customer.fiserv ls.com/ n/a Header missing 2019-01- 22T07:04:02.789Z x_xss_protection_mis https://intranet1.fiservl s.com/ n/a Header missing 2019-01- 22T07:04:02.784Z x_xss_protection_mis https://intranet1.fiservl s.com/ n/a Header missing 2019-01- 22T07:04:02.756Z x_xss_protection_mis http://atlanta.fiservls.c om/ n/a Header missing 2019-01- 22T07:04:02.748Z x_xss_protection_mis https://18.fiservls.com/ https://18.fiservls.com/ n/a Header missing 2019-01-	x_xss_protection_mis sing	•	•	n/a	Header missing	
sing m/ m/ m/ 22T07:04:02.789Z x_xss_protection_mis sing https://customer.fiserv s.com/ https://customer.fiservl s.com/ n/a Header missing 2019-01-22T07:04:02.784Z x_xss_protection_mis https://intranet1.fiservl s.com/ n/a Header missing 2019-01-22T07:04:02.756Z x_xss_protection_mis http://atlanta.fiservls.c om/ http://atlanta.fiservls.c om/ n/a Header missing 2019-01-22T07:04:02.748Z x_xss_protection_mis https://18.fiservls.com/ https://18.fiservls.com/ n/a Header missing 2019-01-	x_xss_protection_mis sing		http://corp.fiservls.com /	n/a	Header missing	
sing Is.com/ s.com/ 22T07:04:02.784Z x_xss_protection_mis s.com/ https://intranet1.fiservl s.com/ n/a Header missing 2019-01- 22T07:04:02.756Z x_xss_protection_mis http://atlanta.fiservls.c om/ n/a Header missing 2019-01- 22T07:04:02.756Z x_xss_protection_mis http://atlanta.fiservls.c om/ n/a Header missing 2019-01- 22T07:04:02.748Z	x_xss_protection_mis sing			n/a	Header missing	
sing s.com/ s.com/ 22T07:04:02.756Z x_xss_protection_mis http://atlanta.fiservls.c om/ n/a Header missing 2019-01- 22T07:04:02.756Z Http://atlanta.fiservls.c om/ n/a Header missing 2019-01- 22T07:04:02.748Z	x_xss_protection_mis sing	•	•	n/a	Header missing	
sing om/ om/ 22T07:04:02.748Z x_xss_protection_mis https://18.fiservls.com/ https://18.fiservls.com/ n/a Header missing 2019-01-	x_xss_protection_mis sing	·		n/a	Header missing	
,	x_xss_protection_mis sing	•	· ·	n/a	Header missing	
	x_xss_protection_mis sing	https://18.fiservls.com/	https://18.fiservls.com/	n/a	Header missing	

x_xss_protection_mis sing	http://customer.fiservl s.com/	http://customer.fiservls .com/	n/a	Header missing	2019-01- 22T07:04:02.710Z
x_xss_protection_mis sing	https://administrador.fi servls.com/	https://administrador.fi servls.com/	n/a	Header missing	2019-01- 22T07:04:02.681Z
x_xss_protection_mis sing	http://intranet1.fiservls.com/	http://intranet1.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:02.673Z
x_xss_protection_mis sing	http://18.fiservls.com/	http://18.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.638Z
x_xss_protection_mis sing	http://administrador.fis ervls.com/	http://administrador.fis ervls.com/	n/a	Header missing	2019-01- 22T07:04:02.606Z
x_xss_protection_mis sing	https://backup.fiservls. com/	https://backup.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:02.590Z
x_xss_protection_mis sing	https://apollo.fiservls.c om/	https://apollo.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:02.577Z
x_xss_protection_mis sing	https://manage.fiservl s.com/	https://manage.fiservls .com/	n/a	Header missing	2019-01- 22T07:04:02.496Z
x_xss_protection_mis sing	http://apollo.fiservls.c om/	http://apollo.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:02.487Z
x_xss_protection_mis sing	https://support.fiservls .com/	https://support.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.457Z
x_xss_protection_mis sing	http://manage.fiservls. com/	http://manage.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:02.415Z
x_xss_protection_mis sing	http://support.fiservls.com/	http://support.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:02.382Z
x_xss_protection_mis sing	http://au.fiservls.com/	http://au.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.382Z
x_xss_protection_mis sing	https://email.fiservls.c om/	https://email.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:02.113Z
x_xss_protection_mis sing	https://ad.fiservls.com /	https://ad.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.039Z
x_xss_protection_mis sing	http://email.fiservls.co m/	http://email.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:02.030Z
x_xss_protection_mis sing	https://download.fiser vls.com/	https://download.fiser vls.com/	n/a	Header missing	2019-01- 22T07:04:02.000Z
x_xss_protection_mis sing	http://ad.fiservls.com/	http://ad.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:01.957Z
x_xss_protection_mis sing	https://am.fiservls.com /	https://am.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:01.913Z
x_xss_protection_mis sing	http://am.fiservls.com/	http://am.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:01.824Z
x_xss_protection_mis sing	https://california.fiservl s.com/	https://california.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:01.632Z
x_xss_protection_mis	https://antivirus.fiservl	https://antivirus.fiservl	n/a	Header missing	2019-01-

sing	s.com/	s.com/			22T07:04:01.624Z
x_xss_protection_mis sing	https://ajax.fiservls.co m/	https://ajax.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:01.621Z
x_xss_protection_mis sing	https://mail.fiservls.co m/	https://mail.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:01.617Z
x_xss_protection_mis sing	https://pop.fiservls.co m/	https://pop.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:01.617Z
x_xss_protection_mis sing	http://ajax.fiservls.com /	http://ajax.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:01.560Z
x_xss_protection_mis sing	http://california.fiservls .com/	http://california.fiservls .com/	n/a	Header missing	2019-01- 22T07:04:01.560Z
x_xss_protection_mis sing	http://antivirus.fiservls.com/	http://antivirus.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:01.560Z

RECOMMENDATION

Add the following header to responses from this website: 'X-XSS-Protection: 1; mode=block'

ABOUT THIS ISSUE

The HTTP X-XSS-Protection response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks. Although these protections are largely unnecessary in modern browsers when websites implement a strong Content-Security-Policy that disables the use of inline JavaScript ('unsafe-inline'), they can still provide protections for users of older web browsers that don't yet support CSP. Without these protections, an attacker can send their victims malicious URLs that inject code into the website

APPLICATION SECURITY > ISSUE DETAIL

Website does not implement X-Content-Type-Options Best Discretions

Practices

-0.3 SCORE

Browsers will sometimes analyze the content themselves and handle it counter to the MIME type header; this can lead to security issues and execution of malicious code. For example, an attacker could hide malicious code with an image extension, where the browser does introspection and executes it as JavaScript.

138 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
x_content_type_optio ns_missing	https://staging.fiserv- ecomhosting.com/	https://staging.fiserv- ecomhosting.com/	n/a	Header missing	2019-01- 29T09:11:43.731Z
x_content_type_optio ns_missing	http://staging.fiserv- ecomhosting.com/	http://staging.fiserv- ecomhosting.com/	n/a	Header missing	2019-01- 29T09:11:43.673Z
x_content_type_optio ns_missing	http://www.fiservsw.c om/	http://www.fiservsw.co m/	n/a	Header missing	2019-01- 29T09:11:42.823Z
x_content_type_optio	https://mail.fiservlendi	https://mail.fiservlendi	n/a	Header missing	2019-01-

ns_missing	ngsolutions.com/	ngsolutions.com/			29T09:11:17.099Z
x_content_type_optio ns_missing	http://fiservcreditservi ces.com/	http://fiservcreditservi ces.com/	n/a	Header missing	2019-01- 29T09:11:15.569Z
x_content_type_optio ns_missing	https://webmail.fiserv. net/	https://webmail.fiserv. net/	n/a	Header missing	2019-01- 29T09:11:13.849Z
x_content_type_optio ns_missing	http://fiservsw.com/	http://fiservsw.com/	n/a	Header missing	2019-01- 29T09:11:05.384Z
x_content_type_options_missing	https://fiserv.service- now.com/auth_redire ct.do? sysparm_url=https%3 a%2f%2flogin.microso ftonline.com%2fte%2ff iservservicepoint.onm icrosoft.com%2fb2c_1 a_prod_sn_signin%2f samlp%2fsso%2flogin %3fsamlrequest%3dlvl bbptaep0vthdgoxfjvs yssvxvupki2o2hf2sdg 7mszjcdhsr%252fx8a kts%252bwep15896b n7ni3drxq7lopeedphf aznttamr17qsis6his2gf ugfwrld77o5wxyfursv hbdxcy5jboko4iesuab sh25scfj7cpuljuzzvgfz mapubn1s%252b0ktq uboi7lt9gqak4w0haw b1ypr3rqatwaaxhswm yhhwbmeadtctzpwtgx qb4qd2qt3em2ouhxnl 5zhxyoaebsnxwtzkpjo %252f8l6rlwbkihwvrh met9umyn%252b%25 2fwzz6uutfnxyvchlhe qrf4ssyizfy%252buqx quqa5fwzmx5s4ww3tj j3sen2gl0qyhklvoz8o dnirewrkjk4sulfwsvnc g8mlgzpl%252fn%25 2bpinyft8ccj%252f%2 52fst9mbl0pwd4p6p %252bk%252bhdynm iemmv6nd1btbbt5xe4 7ei%252f312sl0uvws8 cs1yrrte7bu61kd68rk7 pzwnbu48yh5s02l32 mfzm6vctvlxjwuwanqj xs%252bq%252ff77% 252baw%253d%253d %26relaystate%3dhttp s%253a%252fravpa ge.do	http://my.carreker.com/	http://my.carreker.com /, 302, https://c3.fiserv.com/, 302, https://servicepoint.fis ervapps.com/, 302, https://fiserv.service-now.com/, 302, https://fiserv.service-now.com/, 302, https://fiserv.service-now.com/auth_redirec t.do? sysparm_url=https%3 A%2F%2Flogin.micros oftonline.com%2Fte% 2Ffiservservicepoint.o nmicrosoft.com%2F82 C_1A_Prod_sn_signin %2Fsamlp%2Fsso%2F login%3FSAMLReques t%3DIVLBbptAEPOVtH dgoXFjVsYSsVXVUpK i2O2hF2sDg7MSzJCd hSR%252FX8AkTS%2 52BWep15896bN7Ni3 dRxq7LOPeEDPHfAzn ttamR17qSis6hls2GFu gFWrlD77O5WxYFUrS VHBdXCy5jBOkO4leS uAbsH25sCfj7cpuLJu ZZVGFZmAPUBn1s%2 52BOktQUBOi7lt9gqA k4WOHAwb1yPR3rqaT waAxhSWmyhHWBmE adTCTzpwtGXQB4Qd 2Qt3Em2OUHXNL5Z HxyOaEBsNxwTZkpjO %252F8L6RLWBKIhW VrhmEt9umYn%252B %252FWZZ6UUTFNX yVchlHEqrF4ssyiZfy% 252BuqxquQA5Fwzm x5S4Ww3TjJ3sEN2Gl OqYhklvoz8ODnlREW RkjK4SuLfwsvnCG8Ml gZPl%252FN%252BPl NYf18ccj%252F%252 FsT9MBL0pwd4P6P% 252BK%252BhdVnml emMV6Nd1bTbbt5xe4 7Ei%252F312sL0uvws 8Cs1yrRef2bU61Kd68r K7pZWNBu48Yh5s02l 32MFZM6VcTVLXjWu wAnQjXs%252BAw%253	Header missing	2019-01- 29T09:11:00.692Z

			D%253D%26RelaySta te%3Dhttps%253A%2 52F%252Ffiserv.servi ce- now.com%252Fnavpa ge.do		
	https://search.carreke r.com/	https://search.carreker .com/	n/a	Header missing	2019-01- 29T09:10:57.094Z
	http://search.carreker. com/	http://search.carreker. com/	n/a	Header missing	2019-01- 29T09:10:57.065Z
	https://careers.carrek er.com/	https://careers.carreke r.com/	n/a	Header missing	2019-01- 29T09:10:56.934Z
	https://mail.billmatrix.c om/	https://mail.billmatrix.c om/	n/a	Header missing	2019-01- 29T09:10:56.928Z
	http://careers.carreker .com/	http://careers.carreker .com/	n/a	Header missing	2019-01- 29T09:10:56.855Z
	https://fiservwebsoluti ons.com/	https://fiservwebsoluti ons.com/	n/a	Header missing	2019-01- 29T09:10:53.876Z
	https://support.fiservat lanta.net/	https://support.fiservat lanta.net/	n/a	Header missing	2019-01- 29T09:10:53.729Z
• • • • • • • • • • • • • • • • • • • •	https://alpha.hepsiian. com/	https://alpha.hepsiian. com/	n/a	Header missing	2019-01- 29T09:10:53.348Z
	https://images.hepsiia n.com/	https://images.hepsiia n.com/	n/a	Header missing	2019-01- 29T09:10:52.534Z
• • • • •	https://fiservsupport.c om/	http://fiservsupport.co m/	http://fiservsupport.co m/, 302, https://fiservsupport.c om/	Header missing	2019-01- 29T09:10:51.744Z
• • • • • • • • • • • • • • • • • • • •	https://fiservlendingso lutions.com/	https://fiservlendingsol utions.com/	n/a	Header missing	2019-01- 29T09:10:50.983Z
	http://fiservlendingsol utions.com/	http://fiservlendingsol utions.com/	n/a	Header missing	2019-01- 29T09:10:50.913Z
	https://fiservipvpn.co m/	https://fiservipvpn.com /	n/a	Header missing	2019-01- 29T09:10:50.584Z
/	http://demo.billmatrix.com/	http://demo.billmatrix. com/	n/a	Header missing	2019-01- 29T09:10:50.447Z
/1 - 1	https://www.fiservlend ingsolutions.com/	https://www.fiservlend ingsolutions.com/	n/a	Header missing	2019-01- 29T09:10:50.369Z
	http://mail.fiservlendin gsolutions.com/	http://mail.fiservlendin gsolutions.com/	n/a	Header missing	2019-01- 29T09:10:50.349Z
	http://www.fiservlendi ngsolutions.com/	http://www.fiservlendi ngsolutions.com/	n/a	Header missing	2019-01- 29T09:10:50.285Z
x_content_type_optio ns_missing	https://fiservcws.com/	https://fiservcws.com/	n/a	Header missing	2019-01- 29T09:10:50.069Z
			https://careers.fiserv.c	Header missing	2019-01-

ns_missing scom/ scom/ scom/ 22T070416.824Z x_content_type_optio_ns_missing http://alabama.fiservis.com/ com/ http://alabama.fiservis.com/ n/a Header missing 2019-01- 22T070416.763Z x_content_type_optio_ns_missing https://en.fiservis.com/ n/a Header missing 2019-01- 22T070416.763Z x_content_type_optio_ns_missing https://shofp.fiservis.com/ n/a Header missing 2019-01- 22T070416.759Z x_content_type_optio_ns_missing https://shofp.fiservis.com/ n/a https://shofp.fiservis.com/ n/a Header missing 2019-01- 22T070416.739Z x_content_type_optio_ns_missing https://shofp.fiservis.com/ n/a https://shofp.fiservis.com/ n/a Header missing 2019-01- 22T070416.742Z x_content_type_optio_ns_missing https://shof.fiservis.com/ n/a https://shof.fiservis.com/ n/a Header missing 2019-01- 22T070416.732Z x_content_type_optio_ns_missing https://shof.fiservis.com/ n/a https://shof.fiservis.com/ n/a Header missing 2019-01- 22T070416.732Z x_content_type_optio_ns_missing http://shof.fiservis.com/ n/a http://shof.fiservis.com/ n/a Header missing 2019-01- 22T070416.691Z x_content_type_optio_ns_missing http://shof.fiservis				http://www.careers.fis erv.com, 301, https://www.careers.fi serv.com/		
ns_missing	x_content_type_optio ns_missing	•	'	n/a	Header missing	
	x_content_type_optio ns_missing	•	•	n/a	Header missing	
ns_missing m/ m/ m/ m/ 22107.04:16.7592 x_content_type_options_ms_missing https://ca.fiservis.com/ ns_missing https://ca.fiservis.com/ nv n/a Header missing 2019-01-22107.04:16.742Z x_content_type_options_missing https://bg.fiservis.com/ ns_missing https://bg.fiservis.com/ nv n/a Header missing 2019-01-22107.04:16.732Z x_content_type_options_missing https://bf.fiservis.com/ ns_missing https://bf.fiservis.com/ n/a n/a Header missing 2019-01-22107.04:16.732Z x_content_type_options_missing http://en.fiservis.com/ ns_missing http://en.fiservis.com/ n/a n/a Header missing 2019-01-22107.04:16.691Z x_content_type_options_missing http://en.fiservis.com/ ns_missing http://en.fiservis.com/ n/a n/a Header missing 2019-01-2107.04:16.691Z x_content_type_options_missing http://blog.fiservis.com/ n/a http://blog.fiservis.com/ n/a n/a Header missing 2019-01-2107.04:16.691Z x_content_type_options_missing http://bf.fiservis.com/ n/a http://bf.fiservis.com/ n/a http://bf.fiservis.com/ n/a Header missing 2019-01-22107.04:16.662Z x_content_type_options_missing	x_content_type_optio ns_missing	https://en.fiservls.com /	https://en.fiservls.com/	n/a	Header missing	
ns_missing x_content_type_optio nv_missing x_content_type_optio	x_content_type_optio ns_missing			n/a	Header missing	
ns_missing m/ m/ m/ m/ m/ 22T07.04:16.7312 x_content_type_optio https://bf.fiservis.com/ https://bf.fiservis.com/ n/a	x_content_type_optio ns_missing	https://ca.fiservls.com/	https://ca.fiservls.com/	n/a	Header missing	
ns_missing / 22107.04:16.726Z x_content_type_optio ns_missing https://bf.fiservls.com/ https://bf.fiservls.com/ n/a Header missing 2019-01- 22107.04:16.715Z x_content_type_optio ns_missing http://en.fiservls.com/ http://en.fiservls.com/ n/a Header missing 2019-01- 22107.04:16.691Z x_content_type_optio ns_missing http://bo.fiservls.com/ http://bo.fiservls.com/ n/a Header missing 2019-01- 22107.04:16.691Z x_content_type_optio ns_missing http://bo.fiservls.com/ http://bo.fiservls.com/ n/a Header missing 2019-01- 22107.04:16.662Z x_content_type_optio ns_missing http://shop.fiservls.com/ http://shop.fiservls.com/ n/a Header missing 2019-01- 22107.04:16.662Z x_content_type_optio ns_missing http://bf.fiservls.com/ http://bf.fiservls.com/ n/a Header missing 2019-01- 22107.04:14.664Z x_content_type_optio ns_missing https://shop.fiservls.com/ https://shop.fiservls.com/ n/a Header missing 2019-01- 22107.04:14.963Z x_content_type_optio ns_missing https://shop.fiservls.com/ https://shop.fiservls.com/ n/a Header missing <td< td=""><td>x_content_type_optio ns_missing</td><td></td><td></td><td>n/a</td><td>Header missing</td><td></td></td<>	x_content_type_optio ns_missing			n/a	Header missing	
ns_missing	x_content_type_optio ns_missing	·	https://bg.fiservls.com/	n/a	Header missing	
ns_missing x_content_type_optio http://ca.fiservis.com/ http://ca.fiservis.com/ n/a Header missing 2019-01- 22T07:04:16.691Z x_content_type_optio http://blog.fiservis.co http://blog.fiservis.com n/a Header missing 2019-01- 22T07:04:16.691Z x_content_type_optio http://blog.fiservis.com/ n/a Header missing 2019-01- 22T07:04:16.677Z x_content_type_optio http://shop.fiservis.com/ http://shop.fiservis.com/ n/a Header missing 2019-01- 22T07:04:16.662Z x_content_type_optio http://shop.fiservis.com/ m/ n/a Header missing 2019-01- 22T07:04:16.662Z x_content_type_optio http://shop.fiservis.com/ http://shop.fiservis.com/ n/a Header missing 2019-01- 22T07:04:16.646Z x_content_type_optio https://ap.fiservis.com/ https://ap.fiservis.com/ n/a Header missing 2019-01- 22T07:04:14.968Z x_content_type_optio https://shop.fiservis.com/ https://in.fiservis.com/ n/a Header missing 2019-01- 22T07:04:14.961Z x_content_type_optio https://ww.fiservis.com/ https://ww.fiservis.com/ n/a Header missing 2019-01- 22T07:04:14.953Z x_content_type_optio https://chat.fiservis.co https://ww.fiservis.co n/a Header missing 2019-01- 22T07:04:14.953Z x_content_type_optio https://chat.fiservis.co https://chat.fiservis.co n/a Header missing 2019-01- 22T07:04:14.953Z x_content_type_optio https://shat.fiservis.co https://chat.fiservis.co n/a Header missing 2019-01- 22T07:04:14.953Z x_content_type_optio https://shat.fiservis.co https://chat.fiservis.co n/a Header missing 2019-01- 22T07:04:14.953Z x_content_type_optio https://shat.fiservis.co https://shat.fiservis.com/ n/a Header missing 2019-01- 22T07:04:14.953Z x_content_type_optio https://shat.fiservis.com/ n/a Header missing 2019-01- 22T07:04:14.953Z x_content_type_optio https://shat.fiservis.com/ n/a Header missing 2019-01- 22T07:04:14.953Z	x_content_type_optio ns_missing	https://bf.fiservls.com/	https://bf.fiservls.com/	n/a	Header missing	
ns_missing x_content_type_optio http://blog.fiservls.co http://blog.fiservls.com n/a Header missing 2019-01-22107:04:16.691Z x_content_type_optio http://bg.fiservls.com/ http://bg.fiservls.com/ n/a Header missing 2019-01-22107:04:16.667Z x_content_type_optio http://shop.fiservls.com http://shop.fiservls.com n/a Header missing 2019-01-22107:04:16.662Z x_content_type_optio http://shop.fiservls.com http://shop.fiservls.com n/a Header missing 2019-01-22107:04:16.662Z x_content_type_optio https://ap.fiservls.com/ https://ap.fiservls.com/ n/a Header missing 2019-01-22107:04:16.646Z x_content_type_optio https://ap.fiservls.com/ https://ap.fiservls.com/ n/a Header missing 2019-01-22107:04:14.968Z x_content_type_optio https://in.fiservls.com/ https://in.fiservls.com/ n/a Header missing 2019-01-22107:04:14.961Z x_content_type_optio https://www.fiservls.com n/a Header missing 2019-01-22107:04:14.955Z x_content_type_optio https://chat.fiservls.com https://chat.fiservls.com n/a Header missing 2019-01-22107:04:14.953Z x_content_type_optio https://spanol.fiservls https://chat.fiservls.com n/a Header missing 2019-01-22107:04:14.953Z x_content_type_optio https://spanol.fiservls https://spanol.fiservls n/a Header missing 2019-01-22107:04:14.953Z	x_content_type_optio ns_missing	http://en.fiservls.com/	http://en.fiservls.com/	n/a	Header missing	
ns_missing m/ / 22T07:04:16.677Z x_content_type_optio ns_missing http://bg.fiservls.com/ ns_missing http://bg.fiservls.com/ http://bg.fiservls.com/ ns_missing http://bhp.fiservls.com/ ns_missing http://bhp.fiservls.com http://bhp.fiservls.com n/a Header missing http://bf.fiservls.com/ ns_missing https://bf.fiservls.com/ ns_missing https://ap.fiservls.com/ ns_missing https://ap.fiservls.com/ ns_missing https://ap.fiservls.com/ ns_missing https://ap.fiservls.com/ n/a Header missing https://ap.fiservls.com/ ns_missing https://in.fiservls.com/ n/a Header missing https://in.fiservls.com/ ns_missing https://ww.fiservls.com/ n/a Header missing https://ww.fiservls.com/ ns_missing https://ww.fiservls.com/ n/a Header missing https://ww.fiservls.com/ ns_missing https://ww.fiservls.com/ n/a Header missing https://ww.fiservls.com/ ns_missing https://chat.fiservls.com/ n/a Header missing https://chat.fiservls.com/ ns_missing https://chat.fiservls.com/ n/a Header missing https://chat.fiservls.com/ ns_missing https://chat.fiservls.com/ n/a Header missing https://chat.fiservls.com/ n/a Header missing 2019-01- 22T07:04:14.953Z x_content_type_optio https://chat.fiservls.com/ n/a Header missing 2019-01- 22T07:04:14.953Z x_content_type_optio https://backend.fiservl https://backend.fiservl n/a Header missing 2019-01- 22T07:04:14.953Z x_content_type_optio https://backend.fiservl https://backend.fiservl n/a Header missing 2019-01- 22T07:04:14.953Z x_content_type_optio https://backend.fiservl https://backend.fiservl n/a Header missing 2019-01- 22T07:04:14.953Z	x_content_type_optio ns_missing	http://ca.fiservls.com/	http://ca.fiservls.com/	n/a	Header missing	
ns_missing x_content_type_optio	x_content_type_optio ns_missing		http://blog.fiservls.com /	n/a	Header missing	
ns_missing m/ m/ m/ m/ m/ 22T07:04:16.662Z x_content_type_optio ns_missing http://bf.fiservls.com/ ns_missing https://ap.fiservls.com/ https://ap.fiservls.com/ ns_missing https://ap.fiservls.com/ ns_missing https://ap.fiservls.com/ https://ap.fiservls.com/ ns_missing https://ap.fiservls.com/ https://ap.fiservls.com/ ns_missing https://in.fiservls.com/ https://in.fiservls.com/ ns_missing https://www.fiservls.com/ ns_missing https://www.fiservls.com/ ns_missing https://www.fiservls.com/ ns_missing https://www.fiservls.com/ ns_missing https://chat.fiservls.com/ ns_missing https://chat.fiservls.com	x_content_type_optio ns_missing	http://bg.fiservls.com/	http://bg.fiservls.com/	n/a	Header missing	
ns_missing x_content_type_optio ns_missing x_content_type_optio ns_missing x_content_type_optio ns_missing x_content_type_optio ns_missing https://in.fiservls.com/ https://in.fiservls.com/ n/a https://in.fiservls.com/ n/a Header missing 2019-01- 22T07:04:14.961Z x_content_type_optio ns_missing https://www.fiservls.com n/a Header missing 2019-01- 22T07:04:14.961Z x_content_type_optio ns_missing https://chat.fiservls.com n/a https://chat.fiservls.com n/a Header missing 2019-01- 22T07:04:14.955Z x_content_type_optio ns_missing https://chat.fiservls.co m/ https://chat.fiservls.com n/a Header missing 2019-01- 22T07:04:14.953Z x_content_type_optio ns_missing https://espanol.fiservls n/a Header missing 2019-01- 22T07:04:14.953Z Accontent_type_optio https://backend.fiservl https://backend.fiservl n/a Header missing 2019-01- 22T07:04:14.953Z	x_content_type_optio ns_missing	,	,	n/a	Header missing	
ns_missing x_content_type_optio ns_missing https://in.fiservls.com/ https://in.fiservls.com/ ns_missing x_content_type_optio ns_missing https://www.fiservls.com https://www.fiservls.com n/a x_content_type_optio ns_missing https://chat.fiservls.com n/a https://chat.fiservls.com n/a https://chat.fiservls.com n/a https://chat.fiservls.com n/a https://chat.fiservls.com n/a Header missing 2019-01- 22T07:04:14.955Z x_content_type_optio nttps://chat.fiservls.com n/a x_content_type_optio nttps://espanol.fiservls n/a https://espanol.fiservls n/a Header missing 2019-01- 22T07:04:14.953Z Accontent_type_optio nttps://espanol.fiservls n/a Header missing 2019-01- 22T07:04:14.953Z	x_content_type_optio ns_missing	http://bf.fiservls.com/	http://bf.fiservls.com/	n/a	Header missing	
ns_missing x_content_type_optio nttps://ww.fiservls.co m/ ns_missing https://ww.fiservls.co https://ww.fiservls.com n/a Header missing x_content_type_optio nttps://chat.fiservls.co m/ ns_missing https://chat.fiservls.co n/a Header missing 2019-01- 22T07:04:14.955Z Header missing 2019-01- 22T07:04:14.953Z Acontent_type_optio nttps://espanol.fiservls n/a Header missing 2019-01- 22T07:04:14.953Z https://espanol.fiservls n/a Header missing 2019-01- 22T07:04:14.953Z	x_content_type_optio ns_missing	https://ap.fiservls.com/	https://ap.fiservls.com/	n/a	Header missing	
ns_missing m/ / 22T07:04:14.955Z x_content_type_optio nttps://chat.fiservls.co m/ n/a Header missing 2019-01- 22T07:04:14.953Z x_content_type_optio nttps://espanol.fiservls https://espanol.fiservls n/a Header missing 2019-01- 22T07:04:14.953Z x_content_type_optio https://espanol.fiservl n/a Header missing 2019-01-	x_content_type_optio ns_missing	https://in.fiservls.com/	https://in.fiservls.com/	n/a	Header missing	
ns_missing m/ m/ 22T07:04:14.953Z x_content_type_optio https://espanol.fiservls https://espanol.fiservls n/a Header missing 2019-01- 22T07:04:14.953Z x_content_type_optio https://backend.fiservl https://backend.fiservl n/a Header missing 2019-01-	x_content_type_optio ns_missing	•	https://ww.fiservls.com /	n/a	Header missing	
ns_missing .com/ .com/ .22T07:04:14.953Z x_content_type_optio https://backend.fiservl https://backend.fiservl n/a Header missing 2019-01-	x_content_type_optio ns_missing	•	•	n/a	Header missing	
	x_content_type_optio ns_missing			n/a	Header missing	
	x_content_type_optio ns_missing	•	· ·	n/a	Header missing	

x_content_type_optio ns_missing	https://arizona.fiservls. com/	https://arizona.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:14.918Z
x_content_type_optio ns_missing	http://ns1.fiservls.com/	http://ns1.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.897Z
x_content_type_optio ns_missing	http://ap.fiservls.com/	http://ap.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.897Z
x_content_type_optio ns_missing	http://ww.fiservls.com/	http://ww.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.897Z
x_content_type_optio ns_missing	http://download.fiservl s.com/	http://download.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:14.897Z
x_content_type_optio ns_missing	http://in.fiservls.com/	http://in.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.878Z
x_content_type_optio ns_missing	http://backend.fiservls .com/	http://backend.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:14.878Z
x_content_type_optio ns_missing	http://espanol.fiservls. com/	http://espanol.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:14.863Z
x_content_type_optio ns_missing	http://forums.fiservls.c om/	http://forums.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:14.853Z
x_content_type_optio ns_missing	http://chat.fiservls.co m/	http://chat.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:14.849Z
x_content_type_optio ns_missing	http://arizona.fiservls.c om/	http://arizona.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:14.849Z
x_content_type_optio ns_missing	https://14.fiservls.com/	https://14.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.091Z
x_content_type_optio ns_missing	https://mobile.fiservls.com/	https://mobile.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.089Z
x_content_type_optio ns_missing	https://sadmin.fiservls. com/	https://sadmin.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:14.085Z
x_content_type_optio ns_missing	https://boston.fiservls. com/	https://boston.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:14.083Z
x_content_type_optio ns_missing	https://developer.fiser vls.com/	https://developer.fiser vls.com/	n/a	Header missing	2019-01- 22T07:04:14.073Z
x_content_type_optio ns_missing	https://act.fiservls.com /	https://act.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:14.070Z
x_content_type_optio ns_missing	https://arlington.fiservl s.com/	https://arlington.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:14.063Z
x_content_type_optio ns_missing	https://client.fiservls.c om/	https://client.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:14.063Z
x_content_type_optio ns_missing	https://ftp.fiservls.com /	https://ftp.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.047Z
x_content_type_optio ns_missing	http://mobile.fiservls.c om/	http://mobile.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:14.017Z
x_content_type_optio	http://14.fiservls.com/	http://14.fiservls.com/	n/a	Header missing	2019-01-

ns_missing					22T07:04:14.016Z
ns_missing					22107.04.14.0102
x_content_type_optio ns_missing	http://boston.fiservls.c om/	http://boston.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:14.015Z
x_content_type_optio ns_missing	http://sadmin.fiservls.c om/	http://sadmin.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:14.014Z
x_content_type_optio ns_missing	http://developer.fiserv ls.com/	http://developer.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:13.993Z
x_content_type_optio ns_missing	http://act.fiservls.com/	http://act.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:13.993Z
x_content_type_optio ns_missing	http://client.fiservls.co m/	http://client.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:13.990Z
x_content_type_optio ns_missing	http://backup.fiservls.c om/	http://backup.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:13.984Z
x_content_type_optio ns_missing	http://ftp.fiservls.com/	http://ftp.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:13.780Z
x_content_type_optio ns_missing	https://blackberry.fiser vls.com/	https://blackberry.fiser vls.com/	n/a	Header missing	2019-01- 22T07:04:13.296Z
x_content_type_optio ns_missing	https://citrix.fiservls.co m/	https://citrix.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:13.214Z
x_content_type_optio ns_missing	https://arkansas.fiservl s.com/	https://arkansas.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:13.209Z
x_content_type_optio ns_missing	https://biz.fiservls.com /	https://biz.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:13.207Z
x_content_type_optio ns_missing	http://citrix.fiservls.co m/	http://citrix.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:13.145Z
x_content_type_optio ns_missing	http://biz.fiservls.com/	http://biz.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:13.145Z
x_content_type_optio ns_missing	http://arkansas.fiservls .com/	http://arkansas.fiservls .com/	n/a	Header missing	2019-01- 22T07:04:13.145Z
x_content_type_optio ns_missing	http://blackberry.fiserv ls.com/	http://blackberry.fiserv ls.com/	n/a	Header missing	2019-01- 22T07:04:13.145Z
x_content_type_optio ns_missing	https://demo.fiservls.c om/	https://demo.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:12.891Z
x_content_type_optio ns_missing	https://survey.fiservls. com/	https://survey.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:12.891Z
x_content_type_optio ns_missing	https://au.fiservls.com/	https://au.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:12.849Z
x_content_type_optio ns_missing	http://survey.fiservls.c om/	http://survey.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:12.815Z
x_content_type_optio ns_missing	http://demo.fiservls.co m/	http://demo.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:12.815Z
x_content_type_optio ns_missing	http://arlington.fiservls .com/	http://arlington.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:05.405Z

x_content_type_optio ns_missing	http://fiservdox.com/	http://fiservdox.com/	n/a	Header missing	2019-01- 22T07:04:03.821Z
x_content_type_optio ns_missing	https://team.fiservls.co m/	https://team.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:03.075Z
x_content_type_optio ns_missing	https://ac.fiservls.com/	https://ac.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:03.053Z
x_content_type_optio ns_missing	http://mail.fiservls.com /	http://mail.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:03.030Z
x_content_type_optio ns_missing	http://team.fiservls.co m/	http://team.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:03.013Z
x_content_type_optio ns_missing	https://ns1.fiservls.com /	https://ns1.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:03.005Z
x_content_type_optio ns_missing	https://131.fiservls.com /	https://131.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:02.976Z
x_content_type_optio ns_missing	http://ac.fiservls.com/	http://ac.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.968Z
x_content_type_optio ns_missing	https://forums.fiservls. com/	https://forums.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.940Z
x_content_type_optio ns_missing	http://pop.fiservls.com /	http://pop.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:02.920Z
x_content_type_optio ns_missing	https://corp.fiservls.co m/	https://corp.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:02.904Z
x_content_type_optio ns_missing	http://131.fiservls.com/	http://131.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.897Z
x_content_type_optio ns_missing	https://apps.fiservls.co m/	https://apps.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:02.857Z
x_content_type_optio ns_missing	https://atlanta.fiservls. com/	https://atlanta.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:02.851Z
x_content_type_optio ns_missing	http://corp.fiservls.co m/	http://corp.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:02.819Z
x_content_type_optio ns_missing	http://apps.fiservls.co m/	http://apps.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:02.789Z
x_content_type_optio ns_missing	https://customer.fiserv ls.com/	https://customer.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:02.784Z
x_content_type_optio ns_missing	https://intranet1.fiservl s.com/	https://intranet1.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:02.756Z
x_content_type_optio ns_missing	http://atlanta.fiservls.c om/	http://atlanta.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:02.748Z
x_content_type_optio ns_missing	https://18.fiservls.com/	https://18.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.716Z
x_content_type_optio ns_missing	http://customer.fiservl s.com/	http://customer.fiservls .com/	n/a	Header missing	2019-01- 22T07:04:02.710Z
x_content_type_optio	https://administrador.fi	https://administrador.fi	n/a	Header missing	2019-01-

ne missing	conds com/	conds com/			22T07:04:02.681Z
ns_missing	servls.com/	servls.com/			22107:04:02.6812
x_content_type_optio ns_missing	http://intranet1.fiservls. com/	http://intranet1.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:02.673Z
x_content_type_optio ns_missing	http://18.fiservls.com/	http://18.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.638Z
x_content_type_optio ns_missing	http://administrador.fis ervls.com/	http://administrador.fis ervls.com/	n/a	Header missing	2019-01- 22T07:04:02.606Z
x_content_type_optio ns_missing	https://backup.fiservls. com/	https://backup.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:02.590Z
x_content_type_optio ns_missing	https://apollo.fiservls.c om/	https://apollo.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:02.577Z
x_content_type_optio ns_missing	https://manage.fiservl s.com/	https://manage.fiservls .com/	n/a	Header missing	2019-01- 22T07:04:02.496Z
x_content_type_optio ns_missing	http://apollo.fiservls.c om/	http://apollo.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:02.487Z
x_content_type_optio ns_missing	https://support.fiservls .com/	https://support.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.457Z
x_content_type_optio ns_missing	http://manage.fiservls. com/	http://manage.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:02.415Z
x_content_type_optio ns_missing	http://au.fiservls.com/	http://au.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.382Z
x_content_type_optio ns_missing	http://support.fiservls.com/	http://support.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:02.382Z
x_content_type_optio ns_missing	https://email.fiservls.c om/	https://email.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:02.113Z
x_content_type_optio ns_missing	https://ad.fiservls.com /	https://ad.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.039Z
x_content_type_optio ns_missing	http://email.fiservls.co m/	http://email.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:02.030Z
x_content_type_optio ns_missing	https://download.fiser vls.com/	https://download.fiser vls.com/	n/a	Header missing	2019-01- 22T07:04:02.000Z
x_content_type_optio ns_missing	http://ad.fiservls.com/	http://ad.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:01.957Z
x_content_type_optio ns_missing	https://am.fiservls.com /	https://am.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:01.913Z
x_content_type_optio ns_missing	http://am.fiservls.com/	http://am.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:01.824Z
x_content_type_optio ns_missing	https://california.fiservl s.com/	https://california.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:01.632Z
x_content_type_optio ns_missing	https://antivirus.fiservl s.com/	https://antivirus.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:01.624Z
x_content_type_optio ns_missing	https://ajax.fiservls.co m/	https://ajax.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:01.621Z

x_content_type_optio ns_missing	https://pop.fiservls.co m/	https://pop.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:01.617Z
x_content_type_optio ns_missing	https://mail.fiservls.co m/	https://mail.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:01.617Z
x_content_type_optio ns_missing	http://antivirus.fiservls.com/	http://antivirus.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:01.560Z
x_content_type_optio ns_missing	http://ajax.fiservls.com /	http://ajax.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:01.560Z
x_content_type_optio ns_missing	http://california.fiservls .com/	http://california.fiservls .com/	n/a	Header missing	2019-01- 22T07:04:01.560Z

RECOMMENDATION

Add the following header to responses from this website: $\mbox{'X-}$ Content-Type-Options: nosniff

ABOUT THIS ISSUE

A MIME type is an HTTP header that indicates the type of content returned in a response and how it should be handled and displayed by the browser. Browsers will sometimes analyze the content themselves and handle it counter to the MIME type header; this can lead to security issues and execution of malicious code. The X-Content-Type-Options header indicates that browsers should always trust the declared MIME type from the server and not attempt to analyze the content themselves.

APPLICATION SECURITY > ISSUE DETAIL

✓ Web Application Firewall (WAF) Detected

A web application firewall (WAF) monitors traffic to and from a web application, and attempts to detect and block traffic associated with common malicious behaviors. A WAF is an important defensive layer that helps secure your web application.

6 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
barracuda_applicatio n_firewall	https://mail.efiserv.co m/	https://mail.efiserv.co m/	n/a	-	2019-01- 29T09:11:04.792Z
Evidence: Barracuda Application Fire	wall detected with 25% confic	dence.			
barracuda_applicatio n_firewall	https://www.efiserv.co m/	https://www.efiserv.co m/	n/a	-	2019-01- 29T09:11:04.467Z
Evidence: Barracuda Application Fire	wall detected with 25% confid	dence.			
f5_big_ip_ltm	https://fiserv.service- now.com/auth_redire ct.do? sysparm_url=https%3 a%2f%2flogin.microso ftonline.com%2fte%2ff iservservicepoint.onm icrosoft.com%2fb2c_1	http://my.carreker.com /	http://my.carreker.com /, 302, https://c3.fiserv.com/, 302, https://servicepoint.fis ervapps.com/, 302, https://fiserv.service- now.com/, 302,	-	2019-01- 29T09:11:00.692Z

	a_prod_sn_signin%2f samlp%2fsso%2flogin %3fsamlrequest%3dlvl bbptaep0vthdgoxfjvs yssvxvupki2o2hf2sdg 7mszjcdhsr%252fx8a kts%252bwep15896b n7ni3drxq7lopeedphf aznttamr17qsis6his2gf ugfwrld77o5wxyfursv hbdxcy5jboko4iesuab sh25scfj7cpuljuzzvgfz mapubn1s%252b0ktq uboi7lt9gqak4w0haw b1ypr3rqatwaaxhswm yhhwbmeadtctzpwtgx qb4qd2qt3em2ouhxnl 5zhxyoaebsnxwtzkpjo %252f8l6rlwbkihwvrh met9umyn%252b%25 2fwzz6uutfnxyvchlhe qrf4ssyizfy%252buqx quqa5fwzmx5s4ww3tj j3sen2gl0qyhklvoz8o dnirewrkjk4sulfwsvnc g8mlgzpl%252fn%25 2bpinyft8ccj%252f%2 52fst9mbl0pwd4p6p %252bk%252bhdynm iemmv6nd1btbbt5xe4 7ei%252f312sl0uvws8 cs1yrrte7bu61kd68rk7 pzwnbu48yh5s02l32 mfzm6vctvlxjwuwanqj xs%252bq%252fd77% 252baw%253d%253d %26relaystate%3dhttp s%253a%252fnavpa ge.do		https://fiserv.service- now.com/auth_redirec t.do? sysparm_url=https%3 A%2F%2Flogin.micros oftonline.com%2Fte% 2Ffiservservicepoint.o nmicrosoft.com%2FB2 C_1A_Prod_sn_signin %2Fsamlp%2Fsso%2F login%3FSAMLReques t%3DIVLBbptAEPOVtH dgoXFjVsYSsVXVUpK i2O2hF2sDg7MSzJCd hSR%252FX8AkTS%2 52BWep15896bN7Ni3 dRxq7LOPeEDPHfAzn ttamR17qSis6hls2GFu gFWrlD77O5WxYFUrS VHBdXCy5jBOkO4leS uAbsH25sCfj7cpuLJu zZVGFZmAPUBn1s%2 52B0ktQUBOi7lt9gqA k4W0HAwb1yPR3rqaT waAxhSWmyhHWBmE adTCTzpwtGXQB4Qd 2Qt3Em2OUHXNL5Z HxyOaEBsNxwTZkpjO %252F8L6RLWBKIhW VrhmEt9umYn%252B %252FWZZ6UUTFNX yVchlHEqrF4ssyiZfy% 252BuqxquQA5Fwzm x5S4Ww3TjJ3sEN2Gl OqYhklvoz8ODnIREW RkjK4SuLfwsvnCG8Ml gZPl%252FN%252BPI NYfT8ccj%252F%252 FsT9MBL0pwd4P6P% 252BK%252BhdYnml emMV6Nd1bTbbt5xe4 7Ei%252F312sL0uvws 8Cs1yrRte7bU61Kd68r K7pZWNBu48Yh5s02l 32MFZM6VcTVLXjWu wAnQjXs%252Bq%25 2FD77%252BAw%253 D%253D%26RelaySta te%3Dhttps%253A%2 52F%252Ffiserv.servi ce- now.com%252Fnavpa ge.do		
Evidence: F5 BIG-IP LTM detected wit	h 25% confidence.				
citrix_netscaler	https://my.carreker.co m/login.asp	https://my.carreker.co m/	https://my.carreker.co m/, 302, https://my.carreker.co m/Login.asp	-	2019-01- 29T09:10:59.822Z
Evidence: Citrix NetScaler detected w	ith 25% confidence.				
citrix_netscaler	https://fiservdm.net/vp n/index.html	https://fiservdm.net/	https://fiservdm.net/, 302,	-	2019-01- 29T09:10:55.671Z

			https://fiservdm.net/vp n/index.html	
Evidence: Citrix NetScaler detected v	with 25% confidence.			
citrix_netscaler	https://fiservdmdr.net/ vpn/index.html	https://fiservdmdr.net/	https://fiservdmdr.net/, - 302, https://fiservdmdr.net/ vpn/index.html	2019-01- 29T09:10:49.321Z
Evidence: Citrix NetScaler detected v	with 25% confidence.			

RECOMMENDATION

Companies should consider implementing a web application firewall that can protect against common web vulnerabilities, such as SQL Injection and cross-site scripting (XSS). Many hosting providers offer WAF capabilities as well.

ABOUT THIS ISSUE

A well configured WAF can detect and block a wide variety of attacks. Capabilities vary between products, but at minimum most WAFs can block SQL injection and Cross Site Scripting attacks. A WAF is no substitute to a well-designed web application that is not vulnerable to these attacks in the first place, but it still plays an important roll in providing layered security.

APPLICATION SECURITY > ISSUE DETAIL

Content Security Policy (CSP) Missing

A Content Security Policy (CSP) directive tells a web browser what locations it can load resources from when rendering a webpage. This helps prevent mistaken or malicious resources from being injected into a webpage (and then executed by a user's browser).

145 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
csp_no_policy	https://staging.fiserv- ecomhosting.com/	https://staging.fiserv- ecomhosting.com/	n/a	-	2019-01- 29T09:11:43.731Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://services.fiserv- ecomhosting.com/	http://services.fiserv- ecomhosting.com/	n/a	-	2019-01- 29T09:11:43.673Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://staging.fiserv- ecomhosting.com/	http://staging.fiserv- ecomhosting.com/	n/a	-	2019-01- 29T09:11:43.673Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://www.fiservsw.c om/	http://www.fiservsw.co m/	n/a	-	2019-01- 29T09:11:42.823Z
Evidence: No content security policy	directives found.				

			,		0040.04	
csp_no_policy	https://mail.fiservlendi ngsolutions.com/	https://mail.fiservlendi ngsolutions.com/	n/a	-	2019-01- 29T09:11:17.099Z	
Evidence: No content security policy	directives found.					
csp_no_policy	http://fiservcreditservi ces.com/	http://fiservcreditservi ces.com/	n/a	-	2019-01- 29T09:11:15.569Z	
Evidence: No content security policy directives found.						
csp_no_policy	https://webmail.fiserv. net/	https://webmail.fiserv. net/	n/a	-	2019-01- 29T09:11:13.849Z	
Evidence: No content security policy	directives found.					
csp_no_policy	http://fiservsw.com/	http://fiservsw.com/	n/a	-	2019-01- 29T09:11:05.384Z	
Evidence: No content security policy	directives found.					
csp_no_policy	https://fiserv.service-now.com/auth_redire ct.do? sysparm_url=https%3 a%2f%2flogin.microso ftonline.com%2fte%2ff iservservicepoint.onm icrosoft.com%2fb2c_1 a_prod_sn_signin%2f samlp%2fsso%2flogin %3fsamlrequest%3dlvl bbptaep0vthdgoxfjvs yssvxvupki2o2hf2sdg 7mszjcdhsr%252fx8a kts%252bwep15896b n7ni3drxq7lopeedphf aznttamr17qsis6his2gf ugfwrld77o5wxyfursv hbdxcy5jboko4iesuab sh25scfj7cpuljuzzvgfz mapubn1s%252b0ktq uboi7lt9gqak4w0haw b1ypr3rqatwaaxhswm yhhwbmeadtctzpwtgx qb4qd2qt3em2ouhxnl 5zhxyoaebsnxwtzkpjo %252f8l6rlwbkihwvrh met9umyn%252b%25 2fwzzGuutfnxyvchlhe qrf4ssyizfy%252buqx quqa5fwzmx5s4ww3tj j3sen2gl0qyhklvoz8o dnirewrkjk4sulfwsvnc g8mlgzpl%252fn%25 2bpinyft8ccj%252f%2 52fst9mbl0pwd4p6p %252bk%252bhdynm iemmv6nd1btbbt5xe4 7ei%252f312sl0uvws8 cs1yrrte7bu61kd68rk7 pzwnbu48yh5s02l32 mfzm6vctvlxjwuwanqj xs%252bq%253dd*253d	http://my.carreker.com	http://my.carreker.com /, 302, https://c3.fiserv.com/, 302, https://servicepoint.fis ervapps.com/, 302, https://fiserv.service-now.com/, 302, https://fiserv.service-now.com/, 302, https://fiserv.service-now.com/, 302, https://fiserv.service-now.com/, 302, https://fiserv.service-now.com/, 302, https://fiserv.service-now.com/auth_redirec t.do? sysparm_url=https%3 A%2F%2Flogin.micros oftonline.com%2Fte% 2Ffiservservicepoint.onmicrosoft.com%2F82 C_1A_Prod_sn_signin %2Fsamlp%2Fsso%2F login%3FSAMLReques t%3DIVLBbptAEP0VtH dgoXFjVsYSsVXVUpK i2O2hF2sDg7MSzJCd hSR%252FX8AkTS%2 52BWep15896bN7Ni3 dRxq7LOPeEDPHfAzn ttamR17qSis6hls2GFu gFWrID77O5WxYFUrS VHBdXCy5jBOkO4leS uAbsH25sCfj7cpuLJu ZZVGFZmAPUBn1s%2 52BOktQUBOi7lt9gqA k4WOHAwb1yPR3rqaT waAxhSWmyhHWBmE adTCTzpwtGXQB4Qd 2Qt3Em2OUHXNL5Z HxyOaEBsNxwTZkpjO %252F8L6RLWBKIhW VrhmEt9umYn%252B %252FWZZGUUTFNX yVchlHEqrF4ssyiZfy% 252BuqxquQA5Fwzm x5S4Ww3TjJ3sEN2Gl OqYhklvoz8ODnIREW RkjK4SuLfwsvnCG8MI		2019-01- 29T09:11:00.692Z	

	%26relaystate%3dhttp s%253a%252f%252ffi serv.service- now.com%252fnavpa ge.do		gZPI%252FN%252BPI NYfT8ccj%252F%252 FsT9MBL0pwd4P6P% 252BK%252BhdYnml emMV6Nd1bTbbt5xe4 7Ei%252F312sL0uvws 8Cs1yrRte7bU61Kd68r K7pZWNBu48Yh5s02I 32MFZM6VcTVLXjWu wAnQjXs%252Bq%25 2FD77%252BAw%253 D%253D%26RelaySta te%3Dhttps%253A%2 52F%252Ffiserv.servi ce- now.com%252Fnavpa ge.do		
Evidence: No content security policy	directives found.				
csp_no_policy	https://search.carreke r.com/	https://search.carreker .com/	n/a	-	2019-01- 29T09:10:57.094Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://search.carreker. com/	http://search.carreker. com/	n/a	-	2019-01- 29T09:10:57.065Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://careers.carrek er.com/	https://careers.carreke r.com/	n/a	-	2019-01- 29T09:10:56.934Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://mail.billmatrix.c om/	https://mail.billmatrix.c om/	n/a	-	2019-01- 29T09:10:56.928Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://careers.carreker .com/	http://careers.carreker .com/	n/a	-	2019-01- 29T09:10:56.855Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://fiserv- ecomhosting.com/log on.asp	https://fiserv- ecomhosting.com/	https://fiserv- ecomhosting.com/, 302, https://fiserv- ecomhosting.com/log on.asp	-	2019-01- 29T09:10:53.901Z
Evidence: block-all-mixed-content					
csp_no_policy	https://fiservwebsoluti ons.com/	https://fiservwebsoluti ons.com/	n/a	-	2019-01- 29T09:10:53.876Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://support.fiservat lanta.net/	https://support.fiservat lanta.net/	n/a	-	2019-01- 29T09:10:53.729Z

Evidence: No content security polic	y directives found.				
csp_no_policy	https://www.fiserv- ecomhosting.com/log on.asp	https://www.fiserv- ecomhosting.com/	https://www.fiserv- ecomhosting.com/, 302, https://www.fiserv- ecomhosting.com/log on.asp	-	2019-01- 29T09:10:53.673Z
Evidence: block-all-mixed-content					
csp_no_policy	https://alpha.hepsiian. com/	https://alpha.hepsiian. com/	n/a	-	2019-01- 29T09:10:53.348Z
Evidence: No content security polic	y directives found.				
csp_no_policy	https://auth01.client-central.com/nidp/idff/s so? requestid=iduqs0f5e4 nosmhposwxxb8jculjy &majorversion=1&min orversion=2&issueinst ant=2019-01- 29t09%3a10%3a52z& providerid=https%3a% 2f%2fwww.client-central.com%3a443% 2fnesp%2fidff%2fmet adata&relaystate=ma %3d%3d&consent=ur n%3aliberty%3aconse nt%3aunavailable&ag appna=clientcentral_h ome&forceauthn=fals e&ispassive=false&na meidpolicy=onetime& protocolprofile=http% 3a%2f%2fprojectlibert y.org%2fprofiles%2fbr ws- art⌖=https%3a% 2f%2fwww.fiserveft.co m%2f&authncontextst atementref=radius%2f token%2furi	https://www.fiserveft.com/	https://www.fiserveft.c om/, 302, https://www.client-central.com:443/nesp/app/plogin? agAppNa=clientCentral_Home&c=radius/to ken/uri⌖=%22htt ps://www.fiserveft.com/%22, 302, https://auth01.client-central.com/nidp/idff/s so? RequestID=idUQS0F5 E4NOSmHPOsWxXB8 jCUJjY&MajorVersion=1&MinorVersion=2&Iss ueInstant=2019-01-29T09%3A10%3A52Z &ProviderID=https%3A%2F%2Fwww.client-central.com%3A443%2Fnesp%2Fidff%2Fme tadata&RelayState=MA%3D%3D&consent=urn%3Aliberty%3Aconsent%3Aunavailable&agAppNa=clientCentral_Home&ForceAuthn=false&IsPassive=false&NameIDPolicy=onetime&ProtocolProfile=http%3A%2F%2Fprojectliberty.org%2Fprofiles%2Fbrws-art⌖=https%3A%2F%2Fwww.fiserveft.com%2F&AuthnContextStatementRef=radius%2Ftoken%2Furi		2019-01- 29T09:10:53.019Z
Evidence: No content security polic	y directives found.				
csp_no_policy	https://images.hepsiia n.com/	https://images.hepsiia n.com/	n/a	-	2019-01- 29T09:10:52.534Z
Evidence:					

No content convity police	u directives found				
No content security policy	y directives found.				
csp_no_policy	https://news.checkfre e.com/	https://news.checkfre e.com/	n/a	-	2019-01- 29T09:10:52.427Z
Evidence: No content security policy	y directives found.				
csp_no_policy	https://www.fiservweb solutions.com	http://fiservwebsolutio ns.com/	http://fiservwebsolutio ns.com/, 301, https://www.fiservweb solutions.com	-	2019-01- 29T09:10:52.406Z
Evidence: block-all-mixed-content					
csp_no_policy	https://fiservsupport.c om/	http://fiservsupport.co m/	http://fiservsupport.co m/, 302, https://fiservsupport.c om/	-	2019-01- 29T09:10:51.744Z
Evidence: No content security policy	y directives found.				
csp_no_policy	https://fiservlendingso lutions.com/	https://fiservlendingsol utions.com/	n/a	-	2019-01- 29T09:10:50.983Z
Evidence: No content security policy	y directives found.				
csp_no_policy	http://fiservlendingsol utions.com/	http://fiservlendingsol utions.com/	n/a	-	2019-01- 29T09:10:50.913Z
Evidence: No content security policy	y directives found.				
csp_no_policy	https://fiservipvpn.co m/	https://fiservipvpn.com /	n/a	-	2019-01- 29T09:10:50.584Z
Evidence: No content security policy	y directives found.				
csp_no_policy	http://demo.billmatrix. com/	http://demo.billmatrix. com/	n/a	-	2019-01- 29T09:10:50.447Z
Evidence: No content security policy	y directives found.				
csp_no_policy	https://www.fiservlend ingsolutions.com/	https://www.fiservlend ingsolutions.com/	n/a	-	2019-01- 29T09:10:50.369Z
Evidence: No content security policy	y directives found.				
csp_no_policy	http://mail.fiservlendin gsolutions.com/	http://mail.fiservlendin gsolutions.com/	n/a	-	2019-01- 29T09:10:50.349Z
Evidence: No content security policy directives found.					
csp_no_policy	http://www.fiservlendi ngsolutions.com/	http://www.fiservlendi ngsolutions.com/	n/a	-	2019-01- 29T09:10:50.285Z
Evidence: No content security policy	y directives found.				
csp_no_policy	https://fiservcws.com/	https://fiservcws.com/	n/a	-	2019-01- 29T09:10:50.069Z

Evidence: No content security policy	directives found.					
csp_no_policy	https://www.careers.fi serv.com/	https://careers.fiserv.c om/	https://careers.fiserv.c om/, 301, http://www.careers.fis erv.com, 301, https://www.careers.fi serv.com/	-	2019-01- 29T09:09:27.681Z	
Evidence: No content security policy	directives found.					
csp_no_policy	https://alabama.fiservl s.com/	https://alabama.fiservl s.com/	n/a	-	2019-01- 22T07:04:16.824Z	
Evidence: No content security policy	directives found.					
csp_no_policy	http://alabama.fiservls. com/	http://alabama.fiservls. com/	n/a	-	2019-01- 22T07:04:16.763Z	
Evidence: No content security policy	directives found.					
csp_no_policy	https://en.fiservls.com /	https://en.fiservls.com/	n/a	-	2019-01- 22T07:04:16.760Z	
Evidence: No content security policy	directives found.					
csp_no_policy	https://blog.fiservls.co m/	https://blog.fiservls.co m/	n/a	-	2019-01- 22T07:04:16.759Z	
Evidence: No content security policy	directives found.					
csp_no_policy	https://ca.fiservls.com/	https://ca.fiservls.com/	n/a	-	2019-01- 22T07:04:16.742Z	
Evidence: No content security policy	directives found.					
csp_no_policy	https://shop.fiservls.co m/	https://shop.fiservls.co m/	n/a	-	2019-01- 22T07:04:16.731Z	
Evidence: No content security policy	directives found.					
csp_no_policy	https://bg.fiservls.com /	https://bg.fiservls.com/	n/a	-	2019-01- 22T07:04:16.726Z	
Evidence: No content security policy	directives found.					
csp_no_policy	https://bf.fiservls.com/	https://bf.fiservls.com/	n/a	-	2019-01- 22T07:04:16.715Z	
Evidence: No content security policy directives found.						
csp_no_policy	http://ca.fiservls.com/	http://ca.fiservls.com/	n/a	-	2019-01- 22T07:04:16.691Z	
Evidence: No content security policy	directives found.					
csp_no_policy	http://en.fiservls.com/	http://en.fiservls.com/	n/a	-	2019-01- 22T07:04:16.691Z	

Evidence: No content security police	y directives found.				
csp_no_policy	http://blog.fiservls.co m/	http://blog.fiservls.com /	n/a	-	2019-01- 22T07:04:16.677Z
Evidence: No content security police	ry directives found.				
csp_no_policy	http://shop.fiservls.co m/	http://shop.fiservls.co m/	n/a	-	2019-01- 22T07:04:16.662Z
Evidence: No content security police	ry directives found.				
csp_no_policy	http://bg.fiservls.com/	http://bg.fiservls.com/	n/a	-	2019-01- 22T07:04:16.662Z
Evidence: No content security police	ry directives found.				
csp_no_policy	http://bf.fiservls.com/	http://bf.fiservls.com/	n/a	-	2019-01- 22T07:04:16.646Z
Evidence: No content security police	ry directives found.				
csp_no_policy	https://ap.fiservls.com/	https://ap.fiservls.com/	n/a	-	2019-01- 22T07:04:14.968Z
Evidence: No content security police	ry directives found.				
csp_no_policy	https://in.fiservls.com/	https://in.fiservls.com/	n/a	-	2019-01- 22T07:04:14.961Z
Evidence: No content security police	ry directives found.				
csp_no_policy	https://ww.fiservls.co m/	https://ww.fiservls.com /	n/a	-	2019-01- 22T07:04:14.955Z
Evidence: No content security police	ry directives found.				
csp_no_policy	https://espanol.fiservls .com/	https://espanol.fiservls .com/	n/a	-	2019-01- 22T07:04:14.953Z
Evidence: No content security police	ry directives found.				
csp_no_policy	https://backend.fiservl s.com/	https://backend.fiservl s.com/	n/a	-	2019-01- 22T07:04:14.953Z
Evidence: No content security policy directives found.					
csp_no_policy	https://chat.fiservls.co m/	https://chat.fiservls.co m/	n/a	-	2019-01- 22T07:04:14.953Z
Evidence: No content security police	y directives found.				
csp_no_policy	https://arizona.fiservls. com/	https://arizona.fiservls. com/	n/a	-	2019-01- 22T07:04:14.918Z
Evidence: No content security polic	y directives found.				

csp_no_policy	http://ap.fiservls.com/	http://ap.fiservls.com/	n/a	-	2019-01- 22T07:04:14.897Z	
Evidence: No content security policy directives found.						
csp_no_policy	http://ww.fiservls.com/	http://ww.fiservls.com/	n/a	-	2019-01- 22T07:04:14.897Z	
Evidence: No content security policy	directives found.					
csp_no_policy	http://ns1.fiservls.com/	http://ns1.fiservls.com/	n/a	-	2019-01- 22T07:04:14.897Z	
Evidence: No content security policy	directives found.					
csp_no_policy	http://download.fiservl s.com/	http://download.fiservl s.com/	n/a	-	2019-01- 22T07:04:14.897Z	
Evidence: No content security policy	directives found.					
csp_no_policy	http://in.fiservls.com/	http://in.fiservls.com/	n/a	-	2019-01- 22T07:04:14.878Z	
Evidence: No content security policy	directives found.					
csp_no_policy	http://backend.fiservls .com/	http://backend.fiservls.com/	n/a	-	2019-01- 22T07:04:14.878Z	
Evidence: No content security policy	directives found.					
csp_no_policy	http://espanol.fiservls. com/	http://espanol.fiservls. com/	n/a	-	2019-01- 22T07:04:14.863Z	
Evidence: No content security policy	directives found.					
csp_no_policy	http://forums.fiservls.c om/	http://forums.fiservls.c om/	n/a	-	2019-01- 22T07:04:14.853Z	
Evidence: No content security policy	directives found.					
csp_no_policy	http://chat.fiservls.co m/	http://chat.fiservls.com /	n/a	-	2019-01- 22T07:04:14.849Z	
Evidence: No content security policy	directives found.					
csp_no_policy	http://arizona.fiservls.c om/	http://arizona.fiservls.c om/	n/a	-	2019-01- 22T07:04:14.849Z	
Evidence: No content security policy	directives found.					
csp_no_policy	https://14.fiservls.com/	https://14.fiservls.com/	n/a	-	2019-01- 22T07:04:14.091Z	
Evidence: No content security policy	directives found.					
csp_no_policy	https://mobile.fiservls.com/	https://mobile.fiservls.com/	n/a	-	2019-01- 22T07:04:14.089Z	

Evidence: No content security policy directives found.					
sp_no_policy	https://sadmin.fiservls.com/	https://sadmin.fiservls.com/	n/a	-	2019-01- 22T07:04:14.085Z
Evidence: No content security policy directives found.					
sp_no_policy	https://boston.fiservls.com/	https://boston.fiservls. com/	n/a	-	2019-01- 22T07:04:14.083Z
vidence: o content security polic	cy directives found.				
sp_no_policy	https://developer.fiser vls.com/	https://developer.fiser vls.com/	n/a	-	2019-01- 22T07:04:14.073Z
vidence: lo content security polic	cy directives found.				
sp_no_policy	https://act.fiservls.com /	https://act.fiservls.com /	n/a	-	2019-01- 22T07:04:14.070Z
vidence: lo content security polic	cy directives found.				
esp_no_policy	https://arlington.fiservl s.com/	https://arlington.fiservl s.com/	n/a	-	2019-01- 22T07:04:14.063Z
Evidence: No content security polic	cy directives found.				
csp_no_policy	https://client.fiservls.c om/	https://client.fiservls.c om/	n/a	-	2019-01- 22T07:04:14.063Z
evidence: No content security polic	cy directives found.				
csp_no_policy	https://ftp.fiservls.com /	https://ftp.fiservls.com/	n/a	-	2019-01- 22T07:04:14.047Z
evidence: No content security polic	cy directives found.				
csp_no_policy	http://mobile.fiservls.c om/	http://mobile.fiservls.c om/	n/a	-	2019-01- 22T07:04:14.017Z
Evidence: No content security polic	cy directives found.				
esp_no_policy	http://14.fiservls.com/	http://14.fiservls.com/	n/a	-	2019-01- 22T07:04:14.016Z
vidence: No content security polic	cy directives found.				
sp_no_policy	http://boston.fiservls.c om/	http://boston.fiservls.c om/	n/a	-	2019-01- 22T07:04:14.015Z
Evidence: No content security polic	cy directives found.				
esp_no_policy	http://sadmin.fiservls.c om/	http://sadmin.fiservls.c om/	n/a	-	2019-01- 22T07:04:14.014Z
evidence: No content security polic	cy directives found.				

con no noliny	http://developer.fiserv	http://do.volonorficoryl	2/0		2019-01-
csp_no_policy	ls.com/	http://developer.fiservl s.com/	n/a	-	22T07:04:13.993Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://act.fiservls.com/	http://act.fiservls.com/	n/a	-	2019-01- 22T07:04:13.993Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://client.fiservls.co m/	http://client.fiservls.co m/	n/a	-	2019-01- 22T07:04:13.990Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://backup.fiservls.c om/	http://backup.fiservls.c om/	n/a	-	2019-01- 22T07:04:13.984Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://ftp.fiservls.com/	http://ftp.fiservls.com/	n/a	-	2019-01- 22T07:04:13.780Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://blackberry.fiser vls.com/	https://blackberry.fiser vls.com/	n/a	-	2019-01- 22T07:04:13.296Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://citrix.fiservls.co m/	https://citrix.fiservls.co m/	n/a	-	2019-01- 22T07:04:13.214Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://arkansas.fiservl s.com/	https://arkansas.fiservl s.com/	n/a	-	2019-01- 22T07:04:13.209Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://biz.fiservls.com /	https://biz.fiservls.com /	n/a	-	2019-01- 22T07:04:13.207Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://citrix.fiservls.co m/	http://citrix.fiservls.co m/	n/a	-	2019-01- 22T07:04:13.145Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://arkansas.fiservls .com/	http://arkansas.fiservls .com/	n/a	-	2019-01- 22T07:04:13.145Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://blackberry.fiserv ls.com/	http://blackberry.fiserv ls.com/	n/a	-	2019-01- 22T07:04:13.145Z

Evidence: No content security police	cy directives found.				
csp_no_policy	http://biz.fiservls.com/	http://biz.fiservls.com/	n/a	-	2019-01- 22T07:04:13.145Z
Evidence: No content security polic	cy directives found.				
csp_no_policy	https://survey.fiservls.	https://survey.fiservls.c	n/a	-	2019-01- 22T07:04:12.891Z
Evidence: No content security polic	cy directives found.				
csp_no_policy	https://demo.fiservls.c	https://demo.fiservls.c	n/a	-	2019-01- 22T07:04:12.891Z
Evidence:		OHI/			22107.04.12.0312
No content security police		https://au.fiservls.com/	n/o		2019-01-
csp_no_policy	https://au.fiservls.com/	Titips://au.fiservis.com/	n/a	-	22T07:04:12.849Z
Evidence: No content security polic	cy directives found.				
csp_no_policy	http://demo.fiservls.co m/	http://demo.fiservls.co m/	n/a	-	2019-01- 22T07:04:12.815Z
vidence: No content security polic	cy directives found.				
csp_no_policy	http://survey.fiservls.c om/	http://survey.fiservls.c om/	n/a	-	2019-01- 22T07:04:12.815Z
Evidence: No content security polic	cy directives found.				
csp_no_policy	https://flagstar- devicemanager- uat.fiservapps.com/	https://flagstar- devicemanager- uat.fiservapps.com/	n/a		2019-01- 22T07:04:09.273Z
Evidence: No content security polic	cy directives found.				
csp_no_policy	http://arlington.fiservls .com/	http://arlington.fiservls. com/	n/a	-	2019-01- 22T07:04:05.405Z
Evidence: No content security polic	cy directives found.				
csp_no_policy	http://fiservdox.com/	http://fiservdox.com/	n/a	-	2019-01- 22T07:04:03.821Z
Evidence: No content security polic	cy directives found.				
csp_no_policy	https://team.fiservls.co m/	https://team.fiservls.co m/	n/a	-	2019-01- 22T07:04:03.075Z
Evidence: No content security polic	cy directives found.				
csp_no_policy	https://ac.fiservls.com/	https://ac.fiservls.com/	n/a	-	2019-01- 22T07:04:03.053Z
Evidence: No content security polic	cy directives found.				

csp_no_policy	http://mail.fiservls.com /	http://mail.fiservls.com /	n/a	-	2019-01- 22T07:04:03.030Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://team.fiservls.co m/	http://team.fiservls.co m/	n/a	-	2019-01- 22T07:04:03.013Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://ns1.fiservls.com /	https://ns1.fiservls.com /	n/a	-	2019-01- 22T07:04:03.005Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://131.fiservls.com /	https://131.fiservls.com /	n/a	-	2019-01- 22T07:04:02.976Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://ac.fiservls.com/	http://ac.fiservls.com/	n/a	-	2019-01- 22T07:04:02.968Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://forums.fiservls.com/	https://forums.fiservls.com/	n/a	-	2019-01- 22T07:04:02.940Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://pop.fiservls.com /	http://pop.fiservls.com /	n/a	-	2019-01- 22T07:04:02.920Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://corp.fiservls.co m/	https://corp.fiservls.co m/	n/a	-	2019-01- 22T07:04:02.904Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://131.fiservls.com/	http://131.fiservls.com/	n/a	-	2019-01- 22T07:04:02.897Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://apps.fiservls.co m/	https://apps.fiservls.co m/	n/a	-	2019-01- 22T07:04:02.857Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://atlanta.fiservls. com/	https://atlanta.fiservls.com/	n/a	-	2019-01- 22T07:04:02.851Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://corp.fiservls.co m/	http://corp.fiservls.com /	n/a	-	2019-01- 22T07:04:02.819Z

Evidence: No content security policy	y directives found.				
csp_no_policy	http://apps.fiservls.co m/	http://apps.fiservls.co m/	n/a	-	2019-01- 22T07:04:02.789Z
Evidence: No content security policy	y directives found.				
csp_no_policy	https://customer.fiserv ls.com/	https://customer.fiservl s.com/	n/a	-	2019-01- 22T07:04:02.784Z
Evidence: No content security policy	y directives found.				
csp_no_policy	https://intranet1.fiservl s.com/	https://intranet1.fiservl s.com/	n/a	-	2019-01- 22T07:04:02.756Z
Evidence: No content security policy	y directives found.				
csp_no_policy	http://atlanta.fiservls.c om/	http://atlanta.fiservls.c om/	n/a	-	2019-01- 22T07:04:02.748Z
Evidence: No content security policy	y directives found.				
csp_no_policy	https://18.fiservls.com/	https://18.fiservls.com/	n/a	-	2019-01- 22T07:04:02.716Z
Evidence: No content security policy	y directives found.				
csp_no_policy	http://customer.fiservl s.com/	http://customer.fiservls .com/	n/a	-	2019-01- 22T07:04:02.710Z
Evidence: No content security policy	y directives found.				
csp_no_policy	https://administrador.fi servls.com/	https://administrador.fi servls.com/	n/a	-	2019-01- 22T07:04:02.681Z
Evidence: No content security policy	y directives found.				
csp_no_policy	http://intranet1.fiservls.com/	http://intranet1.fiservls.com/	n/a	-	2019-01- 22T07:04:02.673Z
Evidence: No content security policy	y directives found.				
csp_no_policy	http://18.fiservls.com/	http://18.fiservls.com/	n/a	-	2019-01- 22T07:04:02.638Z
Evidence: No content security policy	y directives found.				
csp_no_policy	http://administrador.fis ervls.com/	http://administrador.fis ervls.com/	n/a	-	2019-01- 22T07:04:02.606Z
Evidence: No content security policy	y directives found.				
csp_no_policy	https://backup.fiservls. com/	https://backup.fiservls. com/	n/a	-	2019-01- 22T07:04:02.590Z
Evidence: No content security policy	y directives found.				

csp_no_policy	https://apollo.fiservls.c om/	https://apollo.fiservls.c om/	n/a	-	2019-01- 22T07:04:02.577Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://manage.fiservl s.com/	https://manage.fiservls .com/	n/a	-	2019-01- 22T07:04:02.496Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://apollo.fiservls.c om/	http://apollo.fiservls.co m/	n/a	-	2019-01- 22T07:04:02.487Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://support.fiservls .com/	https://support.fiservls.com/	n/a	-	2019-01- 22T07:04:02.457Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://manage.fiservls. com/	http://manage.fiservls. com/	n/a	-	2019-01- 22T07:04:02.415Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://au.fiservls.com/	http://au.fiservls.com/	n/a	-	2019-01- 22T07:04:02.382Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://support.fiservls. com/	http://support.fiservls.c om/	n/a	-	2019-01- 22T07:04:02.382Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://email.fiservls.c om/	https://email.fiservls.c om/	n/a	-	2019-01- 22T07:04:02.113Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://ad.fiservls.com /	https://ad.fiservls.com/	n/a	-	2019-01- 22T07:04:02.039Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://email.fiservls.co m/	http://email.fiservls.co m/	n/a	-	2019-01- 22T07:04:02.030Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://download.fiser vls.com/	https://download.fiser vls.com/	n/a	-	2019-01- 22T07:04:02.000Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://ad.fiservls.com/	http://ad.fiservls.com/	n/a	-	2019-01- 22T07:04:01.957Z

Evidence: No content security policy	directives found.				
csp_no_policy	https://am.fiservls.com /	https://am.fiservls.com /	n/a	-	2019-01- 22T07:04:01.913Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://am.fiservls.com/	http://am.fiservls.com/	n/a	-	2019-01- 22T07:04:01.824Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://california.fiservl s.com/	https://california.fiservl s.com/	n/a	-	2019-01- 22T07:04:01.632Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://antivirus.fiservl s.com/	https://antivirus.fiservl s.com/	n/a	-	2019-01- 22T07:04:01.624Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://ajax.fiservls.co m/	https://ajax.fiservls.co m/	n/a	-	2019-01- 22T07:04:01.621Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://mail.fiservls.co m/	https://mail.fiservls.co m/	n/a	-	2019-01- 22T07:04:01.617Z
Evidence: No content security policy	directives found.				
csp_no_policy	https://pop.fiservls.co m/	https://pop.fiservls.co m/	n/a	-	2019-01- 22T07:04:01.617Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://ajax.fiservls.com /	http://ajax.fiservls.com /	n/a	-	2019-01- 22T07:04:01.560Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://california.fiservls .com/	http://california.fiservls .com/	n/a	-	2019-01- 22T07:04:01.560Z
Evidence: No content security policy	directives found.				
csp_no_policy	http://antivirus.fiservls. com/	http://antivirus.fiservls.com/	n/a	-	2019-01- 22T07:04:01.560Z
Evidence: No content security policy	directives found.				

RECOMMENDATION

Enable CSP headers via your webserver configuration.

ABOUT THIS ISSUE

The Content Security Policy provides a valuable safety net that protects your website from malicious cross-site scripting (XSS) attacks. A well configured policy will stop an attacker attempting to inject their code, or references to other malicious content, into your website. Without a Content Security Policy, it's easy for website developers to make mistakes that allow an attacker to inject content that changes the way the website behaves.

APPLICATION SECURITY > ISSUE DETAIL

Content Security Policy Contains Broad Directives

A Content Security Policy (CSP) directive tells a web browser what locations it can load resources from when rendering a webpage. This helps prevent mistaken or malicious resources from being injected into a webpage (and then executed by a user's browser).

1 finding

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN		
csp_too_broad	https://my.carreker.co m/login.asp	https://my.carreker.co m/	https://my.carreker.co m/, 302, https://my.carreker.co m/Login.asp	-	2019-01- 29T09:10:59.822Z		
Evidence: "frame-ancestors c3.fiserv.com facets.fiserv.com","default-src 'self'; img-src 'self' 'data'; connect-src 'self' 'wss'; report-uri https://report-uri.io/report/URL;"							

RECOMMENDATION

Explicitly specify trusted sources for your script-src and objectsrc policies. Ideally you can use the 'self' directive to limit scripts and objects to only those on your own domain, or you can explicitly specify domains that you trust and rely upon for your site to function.

ABOUT THIS ISSUE

The Content Security Policy (CSP) header can mitigate Cross-Site Scripting (XSS) attacks by prohibiting the browser from loading resources on your page from domains that you don't explicitly trust. However, by using overly broad methods of describing what you trust (ie. 'http:', '**', 'http://**') for your script-src and object-src directives, or your default-src directive in the absence of those directives, this key feature of the CSP header can be bypassed by an attacker.

APPLICATION SECURITY > ISSUE DETAIL

Content Security Policy Contains 'unsafe-*' Directive

A Content Security Policy (CSP) directive tells a web browser what locations it can load resources from when rendering a webpage. This helps prevent mistaken or malicious resources from being injected into a webpage (and then executed by a user's browser).

9 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
				DESCRIPTION	

csp_unsafe_policy http://agility- http://agility- n/a - 2019-01- fiserv.com/ fiserv.com/ 29T09:10:55.566Z

Evidence:

default-src https://ssl.gstatic.com https://www.gstatic.com https://cdnjs.cloudflare.com tagmanager.google.com https://fonts.googleapis.com https://cdn.hypemarks.com www.youtube.com https://players.brightcove.net https://hls.cf.brightcove.com https://fonts.gstatic.com https://fonts.googleapis.com https://cdn.hypemarks.com www.digitalfileshares.com https://brightcove.https://secure.brightcove.com https://secure.brightcove.com https://secure.brightcove.com https://secure.brightcove.com https://secure.brightcove.com https://secure.brightcove.com https://sets.g.doubleclick.net https://www.google.com https://stats.g.doubleclick.net https://www.google-analytics.com https://stats.g.doubleclick.net https://stats.google-analytics.com https://stats.google-com https://stats.google-analytics.com https://stats.google-a

csp_unsafe_policy

https://www.fiserv.co m/industries/creditunions/accountprocessingplatforms/galaxy.aspx http://fiservgalaxy.com/

ky.com/ galaxy.com/, 302, http://www.fiserv.com/ industries/creditunions/accountprocessing-

platforms/galaxy.aspx, 302, https://www.fiserv.com /industries/creditunions/accountprocessingplatforms/galaxy.aspx

http://fiserv-

2019-01-

29T09:10:54.588Z

Evidence:

default-src https://ssl.gstatic.com https://www.gstatic.com https://cdnjs.cloudflare.com tagmanager.google.com https://fonts.googleapis.com https://cdn.hypemarks.com www.youtube.com https://players.brightcove.net https://siphtcove.com https://fonts.googleapis.com https://scnnect.facebook.net www.youtube.com https://players.brightcove.net https://www.fiserv.com https://fonts.googleapis.com https://www.google.ca https://www.google.ca https://www.google.ca https://www.google.ca https://www.google.com https://scure.brightcove.com https://scure.brightcove.com https://scure.brightcove.com https://scure.brightcove.com https://scure.brightcove.com https://scure.brightcove.com https://scure.adnxs.com https://www.google-analytics.com https://scure.adnxs.com https://www.google-analytics.com https://scure.adnxs.com https://www.google-analytics.com https://scure.adnxs.com https://scure.adnxs.com https://www.google-analytics.com https://scure.adnxs.com https://scure.adnxs.com https://spingdom.net https://sinaddheadia-af0801c2bd5e1e5f0dc25.ssl.cf1.rackcdn.com https://scure.adnxs.com https://spingdom.net https://scure.adnxs.com https://spingdom.net https://scure.adnxs.com https://spingdom.net https://sp

csp_unsafe_policy http://bbs.summitsite. http://bbs.summitsite.c n/a - 2019-01com/ om/ 29T09:10:53.790Z

Evidence:

default-src https://ssl.gstatic.com https://www.gstatic.com https://cdnjs.cloudflare.com tagmanager.google.com https://fonts.googleapis.com https://connect.facebook.net www.youtube.com https://players.brightcove.net https://s.cf.brightcove.com https://fonts.gstatic.com https://fonts.googleapis.com https://cdn.hypemarks.com www.digitalfileshares.com https://siphtcove.com https://www.fiserv.com https://ys.zencdn.net https://www.google.ca https://*.addthis.com https://siphtcove.com https://siphtcove.com

csp_unsafe_policy https://www.fiservdox. https://www.fiservdox. n/a - 2019-01com/ com/ 29T09:10:53.470Z

Evidence

default-src https://ssl.gstatic.com https://www.gstatic.com https://cdnjs.cloudflare.com tagmanager.google.com https://ion.fiserv.com https://connect.facebook.net www.youtube.com https://players.brightcove.net https://hls.cf.brightcove.com https://fonts.gstatic.com https://fonts.googleapis.com https://cdn.hypemarks.com www.digitalfileshares.com https://scure.brightcove.hs.llnwd.net www.fiserv.com https://sev.com https://secure.brightcove.com https://secure.brightcove.com https://secure.brightcove.com https://secure.brightcove.com https://secure.brightcove.com https://secure.brightcove.com https://secure.brightcove.com https://secure.brightcove.com https://secure.brightcove.com https://secure.archives.com/lates/thtps://www.google-analytics.com/lates/thtps://secure.archives/thttps://secure.archives/thtps://secure.archives/thtps://secure

https://sjs.bizographics.com https://static.ads-twitter.com https://*.pingdom.net https://snap.licdn.com https://vlog.leadformix.com https://*.facebook.com https://*.twitter.com https://www.google.com https://*.facebook.net https://*.linkedin.com https://*.adnxs.com https://players.brightcove.net https://vjs.zencdn.net https://www.fiserv.com blob: https://www.bizographics.com 'unsafe-inline' 'unsafe-eval'

https://www.bizographics	.com 'unsafe-inline' 'unsafe-e	/al'			
csp_unsafe_policy	http://www.fiservdox.c om/	http://www.fiservdox.c om/	n/a	-	2019-01- 29T09:10:53.412Z
www.youtube.com https://www.digitalfileshares.com https://www.google.com https://*doubleclick.net https://log.leadformix.coeval"; script-src https://taghttps://api.keen.io https://https://www.googletagm.https://sjs.bizographics.com https://www.google.com https://www.bizographics	//players.brightcove.net https:// n https://brightcove.hs.llnwd.n https://secure.brightcove.com ttps://www.google.com https:// m https://www.facebook.com manager.google.com https://s www.fiserv.com https://s.ytim anager.com https://s.ytim om https://static.ads-twitter.co https://*.facebook.net https://* .com 'unsafe-inline' 'unsafe-ev	//hls.cf.brightcove.com https://et www.fiserv.com https://www.https://fl.media.brightcove.com/8174811.fls.doubleclick.net https://secure.adnxs.com httpsi/secure.adnxs.com httpsi/secure.adnxs.com httpsi/secure.adnxs.com httpsi/m.addthisedge.com https://m.addthisedge.com https://*.pingdom.net https://ininkedin.com https://*.adnxs.com/al/	//fonts.gstatic.com https://fo w.fiserv.com https://yis.zen. om data: https://metrics.brig ttps://www.google-analytics os://www.pages05.net https f2a3f802cdf2859af9e-5112: om https://www.tintup.com in https://www.sc.pages05.n //snap.licdn.com https://vloq.com https://players.brightco	https://ion.fiserv.com https://con.nts.googleapis.com https://cdn.lcdn.net https://www.google.ca httcove.com https://edge.api.brig.com https://t.com https://stats.g.c.://*.pingdom.net https://*.linkedi8641de34f0801c2bd5e1e5f0dc2nttps://*.cloudfront.net www.fiseet https://*www.google-analytics.g.leadformix.com https://*.facebuve.net https://vjs.zencdn.net https://vj	hypemarks.com https://-addthis.com ght./v*-addthis.com ght./v*-addthis.com loubleclick.net n.com 'unsafe-inline' 'unsafe- 25.ssl.cfl.rackcdn.com rv.com .com .com .com .com .com bok.com https://*.twitter.com .ss://www.fiserv.com blob:
csp_unsafe_policy	https://sysadmin5- cert.fiserv.com/	https://sysadmin5- cert.fiserv.com/	n/a	-	2019-01- 22T07:02:48.862Z

Evidence:

default-src 'none'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; connect-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' data;; style-src 'self' 'unsafe-inline' 'unsafe-eval';

csp_unsafe_policy	https://sysadmin5.fise	https://sysadmin5.fiser	n/a	-	2019-01-
	rv.com/	v.com/			22T07:02:45.601Z

Evidence:

default-src 'none'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; connect-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' data;; style-src 'self' 'unsafe-inline' 'unsafe-eval';

csp_unsafe_policy	https://sysadmin6-	https://sysadmin6-	n/a	-	2019-01-
	cert.fiserv.com/	cert.fiserv.com/			22T07:02:42.949Z

Evidence:

default-src 'none'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; connect-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' data;; style-src 'self' 'unsafe-inline' 'unsafe-eval';

csp_unsafe_policy	https://sysadmin6.fise rv.com/	https://sysadmin6.fiser v.com/	n/a	-	2019-01- 22T07:02:41.175Z

Evidence:

default-src 'none'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; connect-src 'self' 'unsafe-eval'; img-src 'self' data;; style-src 'self' 'unsafe-inline' 'unsafe-eval';

RECOMMENDATION

Remove the unsafe directives from the content security policy. For trusted resources that must be used inline with HTML, you can use nonces or hashes in your content security policy's source list to mark the resources as trusted. Nonces are randomly generated numbers placed with inline content that you trust. By including the nonce in both the content and the header, the browser knows to trust the script. Example inline script with a nonce: <script nonce=aBFef03ncelOfn39hr3rsatsdfa>alert('Hello, world.');</script> Example policy that allows the inline script to be run without unsafe directives: Content-Security-Policy: script-src 'nonce-aBFef03ncelOfn39hr3rsatsdfa' Warning: For nonces to be effective, they must be randomly regenerated every time the page is loaded. If an attacker can guess the nonce value, the protection is useless. Hashes work similarly to nonces, but only need to be generated once. By taking the hash of a script and including it in the header, it will mark the script as trusted. If the attacker tries to change the script, the hash will change and it will no longer be trusted. Example inline script to be hashed: <script>alert('Hello, world.');</script> Example policy that allows the inline script to be run without unsafe directives: Content-Security-Policy: script-src 'sha256qznLcsROx4GACP2dm0UCKCzCG-HiZ1guq6ZZDob_Tng='

ABOUT THIS ISSUE

The Content Security Policy (CSP) header can mitigate Cross-Site Scripting (XSS) attacks by prohibiting the browser from running code embedded within the HTML of your site. However, the use of unsafe-eval and unsafe-inline policies in the CSP prevent this key safety feature from functioning. These unsafe directives mean that, should the site be vulnerable to XSS or HTML injection attacks, the attacker will be able to inject their own resources directly into the HTML response and have the browser execute them.

APPLICATION SECURITY > ISSUE DETAIL

Website Does Not Implement HSTS Best Practices

Leven if a website is protected with HTTPS, most browsers will still try first to connect to the HTTP version of the website unless explicitly specified. At that moment, visitors to the website are vulnerable to a man-in-the-middle attacker that can prevent them from reaching the HTTPS version of the website they intended to visit and instead divert them to a malicious website. The (expand) HSTS header ensures that, after a user's initial visit to the website, that they will not be susceptible to this man-in-the-middle attack because they will immediately connect to the HTTPS-protected website.

85 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
no_hsts	https://staging.fiserv- ecomhosting.com/	https://staging.fiserv- ecomhosting.com/	n/a	No HSTS header found	2019-01- 29T09:11:43.731Z
Evidence: No Strict-Transport-Secu	rity header found.				
no_hsts	https://mail.fiservlendi ngsolutions.com/	https://mail.fiservlendi ngsolutions.com/	n/a	No HSTS header found	2019-01- 29T09:11:17.099Z
Evidence: No Strict-Transport-Secu	rity header found.				
no_hsts	https://webmail.fiserv. net/	https://webmail.fiserv. net/	n/a	No HSTS header found	2019-01- 29T09:11:13.849Z
Evidence:					

https://my.carreker.co mic. 9019-01-1059-8222 https://my.carreker.co mic. 902-01-1059-8222 https://my.carreker.com/carreke	No Strict-Transport-Security	v header found					
mine mine mine mine mine mine mine mine							
No HSTS header 2019-01- 100-151 100-15	hsts_missing_subdom ain			m/, 302, https://my.carreker.co	includeSubDomains		
Com/	Evidence: Strict-Transport-Security: m	ax-age=157680000					
No. hits https://careers.carreke er.com/ No. https://mail.bilimatrix.c om/ No. https://mail.bilimatrix.c om/ No. https://mail.bilimatrix.c om/ No. https://siservdm.net/ No. htt	no_hsts	·	•	n/a			
Exidence: Severage of the Strict Transport Security Header found. Severage of the Strict Transport Security	Evidence: No Strict-Transport-Security	y header found.					
No Strict-Transport-Security header found. Polytic-Transport-Security h	no_hsts		· ·	n/a			
Solidence:	Evidence: No Strict-Transport-Security	y header found.					
https://fiservdm.net/.pn/index.html https://fiservdm.net/.pn/index.html https://fiservdm.net/.pn/index.html https://fiservdm.net/.pn/index.html https://fiservdm.net/.pn/index.html https://fiservdm.net/.pn/index.html https://fiservdm.net/.pn/index.html https://support.fiservationing.com/.pn/index.html https://support.fiservationing.com/.pn/index.html https://support.fiservationing.com/.pn/index.html https://support.fiservationing.com/.pn/.pn/index.html https://support.fiservationing.com/.pn/.pn/.pn/.pn/.pn/.pn/.pn/.pn/.pn/.pn	no_hsts	•		n/a			
Evidence: Strict-Transport-Security: max-age=157680000 Insts_missing_subdom ain https://support.fiservat lanta.net/ Insts_missing_subdom ain https://fiserv-ecomhosting.com/ on.asp Insts_missing_subdom ain https://fiserv-ecomhosting.com/ on.asp Insts_missing_subdom ain https://fiserv-ecomhosting.com/ ons.com/ Insts_missing_subdom ain https://fiserv-ecomhosting.com/ ons.com/ Insts_missing_subdom ain https://fiserv-ecomhosting.com/ ons.com/ Insts_missing_subdom ain https://fiserv-ecomhosting.com/ ons.com/ Insts_missing_subdom ain	Evidence: No Strict-Transport-Security	y header found.					
https://support.fiservat lanta.net/ https://fiservations.com/ ecomhosting.com/ on.asp https://fiserv-ecomhosting.com/ ecomhosting.com/ on.asp https://fiservation.asp https://servation.asp https://s	hsts_missing_subdom ain		https://fiservdm.net/	302, https://fiservdm.net/vp	includeSubDomains		
anta.net/ anta.n	Evidence: Strict-Transport-Security: m	nax-age=157680000					
https://fiserv-ecomhosting.com/ sopon.asp https://fiservecomhosting.com/ sopon.asp https://fiservebsoluti ons.com/ sopon.asp https://fiservebsoluti ons	hsts_missing_subdom ain			anta.net/, 302, https://support.fiservat	includeSubDomains		
ecomhosting.com/log on.asp ecomhosting.com/ a02, https://fiserv-ecomhosting.com/, 302, https://fiserv-ecomhosting.com/log on.asp Evidence: No Strict-Transport-Security header found. Ino_hsts https://fiservwebsoluti ons.com/ beater found. Ino_hsts https://fiservwebsoluti ons.com/ beater found. Insts_missing_subdom ain https://www.fiserv.com/customer-channel-management/output-solutions/operational-documents-supplies.aspx/ Inttps://fiservdox.com/solutions/operational-documents-supplies.aspx/ ecomhosting.com/, 302, https://fiserv-ecomhosting.com/, 302, https://fiservdox.com/, 302, https	Evidence: Strict-Transport-Security: m	ax-age=31536000					
No Strict-Transport-Security header found. https://fiservwebsoluti ons.com/ https://fiservwebsoluti ons.com/ nos.com/ nos.com/ https://fiservwebsoluti ons.com/ nos.com/ nos.	no_hsts	ecomhosting.com/log	•	ecomhosting.com/, 302, https://fiserv- ecomhosting.com/log			
ons.com/ ons.com/ ons.com/ found 29T09:10:53.876Z Evidence: No Strict-Transport-Security header found. https://www.fiserv.co m/customer-channel- management/output- solutions/operational- documents- supplies.aspx/ ons.com/ found 29T09:10:53.876Z https://fiservdox.com/, 302, includeSubDomains directive /customer-channel- management/output- solutions/operational- documents- supplies.aspx/ found 29T09:10:53.876Z https://fiservdox.com/, 302, includeSubDomains directive 2019-01- 29T09:10:53.684Z	Evidence: No Strict-Transport-Securit	y header found.					
No Strict-Transport-Security header found. Insts_missing_subdom ain	no_hsts	•	'	n/a			
ain m/customer-channel- management/output- solutions/operational- documents- supplies.aspx/ mincludeSubDomains 29T09:10:53.684Z https://www.fiserv.com /customer-channel- management/output- solutions/operational- documents- supplies.aspx/	Evidence: No Strict-Transport-Security header found.						
Evidence:	hsts_missing_subdom ain	m/customer-channel- management/output- solutions/operational- documents-	https://fiservdox.com/	302, https://www.fiserv.com /customer-channel- management/output- solutions/operational- documents-	includeSubDomains		
	Evidence:						

Strict-Transport-Security: ma	ax-age=31536000				
no_hsts	https://www.fiserv- ecomhosting.com/log on.asp	http://www.fiserv- ecomhosting.com/	http://www.fiserv- ecomhosting.com/, 302, http://www.fiserv- ecomhosting.com/log on.asp, 302, https://www.fiserv- ecomhosting.com/log on.asp	No HSTS header found	2019-01- 29T09:10:53.649Z
Evidence: No Strict-Transport-Security	/ header found.				
hsts_missing_subdom ain	https://www.fiservdox. com/	https://www.fiservdox. com/	n/a	Header missing includeSubDomains directive	2019-01- 29T09:10:53.470Z
Evidence: Strict-Transport-Security: ma	ax-age=31536000				
no_hsts	https://alpha.hepsiian. com/	https://alpha.hepsiian. com/	n/a	No HSTS header found	2019-01- 29T09:10:53.348Z
Evidence: No Strict-Transport-Security	y header found.				
hsts_missing_subdom ain	https://auth01.client-central.com/nidp/idff/s so? requestid=idgngcjotb nf60kxgjik8ar7px-qm&majorversion=1&minorversion=2&issue instant=2019-01-29t09%3a10%3a53z&providerid=https%3a%2f%2fwww.client-central.com%3a443%2fnesp%2fidff%2fmet adata&relaystate=ma%3d%3d&consent=urn%3aliberty%3aconsent%3aunavailable&agappna=clientcentral_home&forceauthn=false&ispassive=false&nameidpolicy=onetime&protocolprofile=http%3a%2f%2fprojectliberty.org%2fprofiles%2fbrws-art⌖=https%3a%2f%2fwww.client-central.com%2f&authncontextstatementref=radius%2ftoken%2furi	http://secure.fiserveft.com/	http://secure.fiserveft. com/, 302, https://www.client- central.com/, 302, https://www.client- central.com:443/nesp/ app/plogin? agAppNa=clientCentral_Home&c=radius/to ken/uri⌖=%22htt ps://www.client- central.com/%22, 302, https://auth01.client- central.com/nidp/idff/s so? RequestID=idGNGCJo TbNF60kxgjik8Ar7px- QM&MajorVersion=1& MinorVersion=2&Issue Instant=2019-01- 29T09%3A10%3A53Z &ProviderID=https%3A %2F%2Fwww.client- central.com/3A443% 2Fnesp%2Fidff%2Fme tadata&RelayState=M A%3D%3D&consent=u rn%3Aliberty%3Acons ent%3Aunavailable&a gAppNa=clientCentral _Home&ForceAuthn=f alse&IsPassive=false& NameIDPolicy=onetim e&ProtocolProfile=http %3A%2F%2Fprojectlib erty.org%2Fprofiles%2 Fbrws- art⌖=https%3A% 2F%2Fwww.client- central.com%2F&Auth	Header missing includeSubDomains directive	2019-01- 29T09:10:53.326Z

			nContextStatementRe f=radius%2Ftoken%2F uri		
Evidence: Strict-Transport-Security: m	nax-age=31536000				
no_hsts	https://images.hepsiia n.com/	https://images.hepsiia n.com/	n/a	No HSTS header found	2019-01- 29T09:10:52.534Z
Evidence: No Strict-Transport-Securit	y header found.				
no_hsts	https://news.checkfre e.com/	https://news.checkfre e.com/	n/a	No HSTS header found	2019-01- 29T09:10:52.427Z
Evidence: No Strict-Transport-Securit	y header found.				
no_hsts	https://www.fiservweb solutions.com	http://fiservwebsolutio ns.com/	http://fiservwebsolutio ns.com/, 301, https://www.fiservweb solutions.com	No HSTS header found	2019-01- 29T09:10:52.406Z
Evidence: No Strict-Transport-Securit	y header found.				
hsts_missing_subdom ain	https://fiservsupport.c om/	http://fiservsupport.co m/	http://fiservsupport.co m/, 302, https://fiservsupport.c om/	Header missing includeSubDomains directive	2019-01- 29T09:10:51.744Z
Evidence: Strict-Transport-Security: m	nax-age=31536000				
no_hsts	https://fiservlendingso lutions.com/	https://fiservlendingsol utions.com/	n/a	No HSTS header found	2019-01- 29T09:10:50.983Z
Evidence: No Strict-Transport-Securit	y header found.				
no_hsts	https://fiservipvpn.co m/	https://fiservipvpn.com /	n/a	No HSTS header found	2019-01- 29T09:10:50.584Z
Evidence: No Strict-Transport-Securit	y header found.				
no_hsts	https://www.fiservlend ingsolutions.com/	https://www.fiservlend ingsolutions.com/	n/a	No HSTS header found	2019-01- 29T09:10:50.369Z
Evidence: No Strict-Transport-Securit	y header found.				
no_hsts	https://fiservcws.com/	https://fiservcws.com/	n/a	No HSTS header found	2019-01- 29T09:10:50.069Z
Evidence: No Strict-Transport-Securit	y header found.				
hsts_missing_subdom ain	https://fiservdmdr.net/ vpn/index.html	https://fiservdmdr.net/	https://fiservdmdr.net/, 302, https://fiservdmdr.net/ vpn/index.html	Header missing includeSubDomains directive	2019-01- 29T09:10:49.321Z
Evidence: Strict-Transport-Security: m	nax-age=157680000				
no_hsts	https://www.careers.fi serv.com/	http://careers.fiserv.co m/	http://careers.fiserv.co m/, 301,	No HSTS header found	2019-01- 29T09:09:27.681Z

			http://www.careers.fis erv.com, 301, https://www.careers.fi serv.com/		
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://alabama.fiservl s.com/	https://alabama.fiservl s.com/	n/a	No HSTS header found	2019-01- 22T07:04:16.824Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://en.fiservls.com /	https://en.fiservls.com/	n/a	No HSTS header found	2019-01- 22T07:04:16.760Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://blog.fiservls.co m/	https://blog.fiservls.co m/	n/a	No HSTS header found	2019-01- 22T07:04:16.759Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://ca.fiservls.com/	https://ca.fiservls.com/	n/a	No HSTS header found	2019-01- 22T07:04:16.742Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://shop.fiservls.co m/	https://shop.fiservls.co m/	n/a	No HSTS header found	2019-01- 22T07:04:16.731Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://bg.fiservls.com /	https://bg.fiservls.com/	n/a	No HSTS header found	2019-01- 22T07:04:16.726Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://bf.fiservls.com/	https://bf.fiservls.com/	n/a	No HSTS header found	2019-01- 22T07:04:16.715Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://ap.fiservls.com/	https://ap.fiservls.com/	n/a	No HSTS header found	2019-01- 22T07:04:14.968Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://in.fiservls.com/	https://in.fiservls.com/	n/a	No HSTS header found	2019-01- 22T07:04:14.961Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://ww.fiservls.co m/	https://ww.fiservls.com /	n/a	No HSTS header found	2019-01- 22T07:04:14.955Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://espanol.fiservls	https://espanol.fiservls	n/a	No HSTS header	2019-01-

	.com/	.com/		found	22T07:04:14.953Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://backend.fiservl s.com/	https://backend.fiservl s.com/	n/a	No HSTS header found	2019-01- 22T07:04:14.953Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://chat.fiservls.co m/	https://chat.fiservls.co m/	n/a	No HSTS header found	2019-01- 22T07:04:14.953Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://arizona.fiservls. com/	https://arizona.fiservls. com/	n/a	No HSTS header found	2019-01- 22T07:04:14.918Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://14.fiservls.com/	https://14.fiservls.com/	n/a	No HSTS header found	2019-01- 22T07:04:14.091Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://mobile.fiservls.com/	https://mobile.fiservls.com/	n/a	No HSTS header found	2019-01- 22T07:04:14.089Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://sadmin.fiservls. com/	https://sadmin.fiservls. com/	n/a	No HSTS header found	2019-01- 22T07:04:14.085Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://boston.fiservls.com/	https://boston.fiservls.com/	n/a	No HSTS header found	2019-01- 22T07:04:14.083Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://developer.fiser vls.com/	https://developer.fiser vls.com/	n/a	No HSTS header found	2019-01- 22T07:04:14.073Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://act.fiservls.com /	https://act.fiservls.com /	n/a	No HSTS header found	2019-01- 22T07:04:14.070Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://arlington.fiservl s.com/	https://arlington.fiservl s.com/	n/a	No HSTS header found	2019-01- 22T07:04:14.063Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://client.fiservls.c om/	https://client.fiservls.c om/	n/a	No HSTS header found	2019-01- 22T07:04:14.063Z
Evidence:					

No Strict-Transport-Security	y header found.				
no_hsts	https://ftp.fiservls.com /	https://ftp.fiservls.com/	n/a	No HSTS header found	2019-01- 22T07:04:14.047Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://blackberry.fiser vls.com/	https://blackberry.fiser vls.com/	n/a	No HSTS header found	2019-01- 22T07:04:13.296Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://citrix.fiservls.co m/	https://citrix.fiservls.co m/	n/a	No HSTS header found	2019-01- 22T07:04:13.214Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://arkansas.fiservl s.com/	https://arkansas.fiservl s.com/	n/a	No HSTS header found	2019-01- 22T07:04:13.209Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://biz.fiservls.com /	https://biz.fiservls.com /	n/a	No HSTS header found	2019-01- 22T07:04:13.207Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://survey.fiservls. com/	https://survey.fiservls.c om/	n/a	No HSTS header found	2019-01- 22T07:04:12.891Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://demo.fiservls.c om/	https://demo.fiservls.c om/	n/a	No HSTS header found	2019-01- 22T07:04:12.891Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://au.fiservls.com/	https://au.fiservls.com/	n/a	No HSTS header found	2019-01- 22T07:04:12.849Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://team.fiservls.co m/	https://team.fiservls.co m/	n/a	No HSTS header found	2019-01- 22T07:04:03.075Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://ac.fiservls.com/	https://ac.fiservls.com/	n/a	No HSTS header found	2019-01- 22T07:04:03.053Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://ns1.fiservls.com /	https://ns1.fiservls.com /	n/a	No HSTS header found	2019-01- 22T07:04:03.005Z
Evidence: No Strict-Transport-Securit	y header found.				
no_hsts	https://131.fiservls.com	https://131.fiservls.com	n/a	No HSTS header	2019-01-

	/	/		found	22T07:04:02.976Z
Evidence: No Strict-Transport-Securit	y header found.				
no_hsts	https://forums.fiservls.com/	https://forums.fiservls.com/	n/a	No HSTS header found	2019-01- 22T07:04:02.940Z
Evidence: No Strict-Transport-Securit	y header found.				
no_hsts	https://corp.fiservls.co m/	https://corp.fiservls.co m/	n/a	No HSTS header found	2019-01- 22T07:04:02.904Z
Evidence: No Strict-Transport-Securit	y header found.				
no_hsts	https://apps.fiservls.co m/	https://apps.fiservls.co m/	n/a	No HSTS header found	2019-01- 22T07:04:02.857Z
Evidence: No Strict-Transport-Securit	y header found.				
no_hsts	https://atlanta.fiservls. com/	https://atlanta.fiservls. com/	n/a	No HSTS header found	2019-01- 22T07:04:02.851Z
Evidence: No Strict-Transport-Securit	y header found.				
no_hsts	https://customer.fiserv ls.com/	https://customer.fiservl s.com/	n/a	No HSTS header found	2019-01- 22T07:04:02.784Z
Evidence: No Strict-Transport-Securit	y header found.				
no_hsts	https://intranet1.fiservl s.com/	https://intranet1.fiservl s.com/	n/a	No HSTS header found	2019-01- 22T07:04:02.756Z
Evidence: No Strict-Transport-Securit	y header found.				
no_hsts	https://18.fiservls.com/	https://18.fiservls.com/	n/a	No HSTS header found	2019-01- 22T07:04:02.716Z
Evidence: No Strict-Transport-Securit	y header found.				
no_hsts	https://administrador.fi servls.com/	https://administrador.fi servls.com/	n/a	No HSTS header found	2019-01- 22T07:04:02.681Z
Evidence: No Strict-Transport-Securit	y header found.				
no_hsts	https://backup.fiservls. com/	https://backup.fiservls. com/	n/a	No HSTS header found	2019-01- 22T07:04:02.590Z
Evidence: No Strict-Transport-Securit	y header found.				
no_hsts	https://apollo.fiservls.c om/	https://apollo.fiservls.c om/	n/a	No HSTS header found	2019-01- 22T07:04:02.577Z
Evidence: No Strict-Transport-Securit	y header found.				
no_hsts	https://manage.fiservl s.com/	https://manage.fiservls .com/	n/a	No HSTS header found	2019-01- 22T07:04:02.496Z
Evidence:					

No Strict-Transport-Security	/ header found.				
no_hsts	https://support.fiservls .com/	https://support.fiservls.com/	n/a	No HSTS header found	2019-01- 22T07:04:02.457Z
Evidence: No Strict-Transport-Security	/ header found.				
no_hsts	https://email.fiservls.c om/	https://email.fiservls.c om/	n/a	No HSTS header found	2019-01- 22T07:04:02.113Z
Evidence: No Strict-Transport-Security	/ header found.				
no_hsts	https://ad.fiservls.com /	https://ad.fiservls.com/	n/a	No HSTS header found	2019-01- 22T07:04:02.039Z
Evidence: No Strict-Transport-Security	/ header found.				
no_hsts	https://download.fiser vls.com/	https://download.fiser vls.com/	n/a	No HSTS header found	2019-01- 22T07:04:02.000Z
Evidence: No Strict-Transport-Security	/ header found.				
no_hsts	https://am.fiservls.com /	https://am.fiservls.com /	n/a	No HSTS header found	2019-01- 22T07:04:01.913Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://california.fiservl s.com/	https://california.fiservl s.com/	n/a	No HSTS header found	2019-01- 22T07:04:01.632Z
Evidence: No Strict-Transport-Security	/ header found.				
no_hsts	https://antivirus.fiservl s.com/	https://antivirus.fiservl s.com/	n/a	No HSTS header found	2019-01- 22T07:04:01.624Z
Evidence: No Strict-Transport-Security	/ header found.				
no_hsts	https://ajax.fiservls.co m/	https://ajax.fiservls.co m/	n/a	No HSTS header found	2019-01- 22T07:04:01.621Z
Evidence: No Strict-Transport-Security	y header found.				
no_hsts	https://mail.fiservls.co m/	https://mail.fiservls.co m/	n/a	No HSTS header found	2019-01- 22T07:04:01.617Z
Evidence: No Strict-Transport-Security	/ header found.				
no_hsts	https://pop.fiservls.co m/	https://pop.fiservls.co m/	n/a	No HSTS header found	2019-01- 22T07:04:01.617Z
Evidence: No Strict-Transport-Security	/ header found.				
hsts_missing_subdom ain	https://sysadmin5- cert.fiserv.com/	https://sysadmin5- cert.fiserv.com/	n/a	Header missing includeSubDomains directive	2019-01- 22T07:02:48.862Z
Evidence: Strict-Transport-Security: m	ax-age=31536000				

hsts_missing_subdom ain	https://sysadmin5.fise rv.com/	https://sysadmin5.fiser v.com/	n/a	Header missing includeSubDomains directive	2019-01- 22T07:02:45.601Z
Evidence: Strict-Transport-Security: m	ax-age=31536000				
hsts_missing_subdom ain	https://sysadmin6- cert.fiserv.com/	https://sysadmin6- cert.fiserv.com/	n/a	Header missing includeSubDomains directive	2019-01- 22T07:02:42.949Z
Evidence: Strict-Transport-Security: m	ax-age=31536000				
hsts_missing_subdom ain	https://sysadmin6.fise rv.com/	https://sysadmin6.fiser v.com/	n/a	Header missing includeSubDomains directive	2019-01- 22T07:02:41.175Z
Evidence: Strict-Transport-Security: m	ax-age=31536000				

RECOMMENDATION

Every web application (and any URLs traversed to arrive at the website via redirects) should set the HSTS header to remain in effect for at least 12 months (31536000 seconds). It is also recommended to set the 'includeSubDomains' directive so that requests to subdomains are also automatically upgraded to HTTPS. An acceptable HSTS header would declare: Strict-Transport-Security: max-age=31536000; includeSubDomains;

ABOUT THIS ISSUE

HTTP Strict Transport Security is an HTTP header that instructs clients (e.g., web browsers) to only connect to a website over encrypted HTTPS connections. Clients that respect this header will automatically upgrade all connection attempts from HTTP to HTTPS. After a client receives the HSTS header upon its first website visit, future connections to that website are protected against Man-in-the-Middle attacks that attempt to downgrade to an unencrypted HTTP connection. The browser will expire the HTTP Strict Transport Security header after the number of seconds configured in the max-age attribute.

APPLICATION SECURITY > ISSUE DETAIL

Site does not enforce HTTPS

Site does not enforce the use of HTTPS encryption, leaving the user vulnerable to man-inthe-middle attackers (who can falsify data and inject malicious code). -1.6 SCORE IMPACT

70 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
http_only	http://staging.fiserv- ecomhosting.com/	http://staging.fiserv- ecomhosting.com/	n/a	-	2019-01- 29T09:11:43.673Z
http_only	http://services.fiserv- ecomhosting.com/	http://services.fiserv- ecomhosting.com/	n/a	-	2019-01- 29T09:11:43.673Z
http_only	http://www.fiservsw.c om/	http://www.fiservsw.co m/	n/a	-	2019-01- 29T09:11:42.823Z
http_only	http://fiservcreditservices.com/	http://fiservcreditservices.com/	n/a	-	2019-01- 29T09:11:15.569Z
http_only	http://fiservsw.com/	http://fiservsw.com/	n/a	-	2019-01- 29T09:11:05.384Z

	http_only		•	n/a	-	
fiserv.com/ fiserv.com/ fiserv.com/ com/	http_only	•	•	n/a	-	
Com/	http_only			n/a	-	
om/ om// om// 29T09:10:33.4122 http_only http://fiservlendingsol ultons.com/ http://fiservlendingsol ultons.com/ n/a - 2019-01-29T09:10:50.9132 http_only http://demo.billmatrix.com/ http://demo.billmatrix.com/ n/a - 2019-01-29T09:10:50.0447Z http_only http://mail.fiservlending solutions.com/ http://www.fiservlendin gsolutions.com/ n/a - 2019-01-29T09:10:50.0449Z http_only http://www.fiservlendin gsolutions.com/ http://www.fiservlendin gsolutions.com/ n/a - 2019-01-29T09:10:50.0449Z http_only http://lealabama.fiservls. http://lealabama.fiservls. n/a - 2019-01-29T09:10:50.0452Z http_only http://en.fiservls.com/ http://en.fiservls.com/ n/a - 2019-01-22T07:04:16:69TZ http_only http://en.fiservls.com/ http://sa.fiservls.com/ n/a - 2019-01-22T07:04:16:69TZ http_only http://bg.fiservls.com/ http://sb.g.fiservls.com/ n/a - 2019-01-22T07:04:16:69TZ http_only http://sb.p.fiservls.com/ http://sb.p.fiservls.com/ htt	http_only	•	•	n/a	-	
http_only http://demo.billmatrix. com/	http_only	•	•	n/a	-	
Com/ Com/ Com/ 29T09:10:50.447Z	http_only			n/a	-	
gsolutions.com/ gsolutions.com/ 29109-10-50.3492 2019-01- 2910-10-50.3492 2019-01- 2910-10-50.2852 2019-01- 2910-10-50.2852 2019-01- 2910-10-50.2852 2019-01- 2910-10-50.2852 2019-01- 2019-01	http_only	•	•	n/a	-	
ngsolutions.com/ ngsolutions.com/ 29709:10:50.285z http_only http://alabama.fiserv/s. com/ com/ com/ com/ 2019-01- 22707:04:16.763z http_only http://ea.fiservis.com/ http://ea.fiservis.com/ n/a - 2019-01- 22707:04:16.691z http_only http://ca.fiservis.com/ http://ea.fiservis.com/ n/a - 2019-01- 22707:04:16.691z http_only http://bg.fiservis.com/ http://blog.fiservis.com/ n/a - 2019-01- 22707:04:16.691z http_only http://bg.fiservis.com/ http://bg.fiservis.com/ n/a - 2019-01- 22707:04:16.662z http_only http://shop.fiservis.com/ http://shop.fiservis.com/ n/a - 2019-01- 22707:04:16.662z http_only http://shop.fiservis.com/ http://shop.fiservis.com/ n/a - 2019-01- 22707:04:16.64cz http_only http://ww.fiservis.com/ http://ww.fiservis.com/ n/a - 2019-01- 22707:04:14.64cz http_only http://download.fiservi http://download.fiservi s.com/ s.com/ http://download.fiservi s.com/ http://download.fiservi s.com/ http://ap.fiservis.com/ n/a - 2019-01- 22707:04:14.897z http_only http://ap.fiservis.com/ http://ap.fiservis.com/ n/a - 2019-01- 22707:04:14.897z	http_only	•		n/a	-	
Com/ Com/ Com/ Com/ C2T07:04:16.763Z C2107:04:16.763Z C2107:04:16.763Z C2107:04:16.763Z C2107:04:16.763Z C2107:04:16.691Z C2107:04:16.662Z C2107:04:16.662Z C2107:04:16.662Z C2107:04:16.662Z C2107:04:16.691Z C2	http_only	•	•	n/a	-	
http_only http://ca.fiservis.com/ http://ca.fiservis.com/ n/a - 2019-01-22T07:04:16.6912 http_only http://blog.fiservis.com http://blog.fiservis.com n/a - 2019-01-22T07:04:16.6912 http_only http://bg.fiservis.com/ http://bg.fiservis.com/ n/a - 2019-01-22T07:04:16.6622 http_only http://shop.fiservis.co http://shop.fiservis.co m/ n/a - 2019-01-22T07:04:16.6622 http_only http://shop.fiservis.com/ http://bf.fiservis.com/ n/a - 2019-01-22T07:04:16.6622 http_only http://bf.fiservis.com/ http://bf.fiservis.com/ n/a - 2019-01-22T07:04:16.6462 http_only http://www.fiservis.com/ http://www.fiservis.com/ n/a - 2019-01-22T07:04:14.8972 http_only http://download.fiservi s.com/ s.com/ n/a - 2019-01-22T07:04:14.8972 http_only http://sf.fiservis.com/ http://sf.fiservis.com/ n/a - 2019-01-22T07:04:14.8972 http_only http://sf.fiservis.com/ http://sf.fiservis.com/ n/a - 2019-01-22T07:04:14.8972 http_only http://sf.fiservis.com/ http://sf.fiservis.com/ http://sf.fiservis.com/ http://sf.fiservis.com/ http://sf.fiservis.com/ http://sf.fiservis.com/ n/a - 2019-01-22T07:04:14.8972 http_only http://sf.fiservis.com/ ht	http_only	•	•	n/a	-	
http_only http://blog.fiservls.com // // // // // 22T07:04:16.691Z // 22T07:04:16.691Z // 22T07:04:16.691Z // 22T07:04:16.691Z // 22T07:04:16.677Z // 22T07:04:16.677Z // 22T07:04:16.677Z // 22T07:04:16.677Z // 22T07:04:16.67Z // 22T07:04:16.662Z // 22T07:04:16.646Z // 22T07:04:16.662Z	http_only	http://en.fiservls.com/	http://en.fiservls.com/	n/a	-	
http_only http://bg.fiservis.com/ http://bg.fiservis.com/ n/a 2019-01-22T07:04:16.662Z http_only http://shop.fiservis.co http://shop.fiservis.co n/a 2019-01-22T07:04:16.662Z http_only http://bf.fiservis.com/ http://bf.fiservis.com/ n/a - 2019-01-22T07:04:16.646Z http_only http://ww.fiservis.com/ http://ww.fiservis.com/ n/a - 2019-01-22T07:04:16.646Z http_only http://download.fiservi http://download.fiservi n/a - 2019-01-22T07:04:14.897Z http_only http://download.fiservi http://download.fiservi n/a - 2019-01-22T07:04:14.897Z http_only http://ns1.fiservis.com/ http://ns1.fiservis.com/ n/a - 2019-01-22T07:04:14.897Z http_only http://ap.fiservis.com/ http://ap.fiservis.com/ n/a - 2019-01-22T07:04:14.897Z http_only http://ap.fiservis.com/ http://ap.fiservis.com/ n/a - 2019-01-22T07:04:14.897Z http_only http://ap.fiservis.com/ http://backend.fiservis. n/a - 2019-01-22T07:04:14.897Z http_only http://backend.fiservis. http://backend.fiservis. n/a - 2019-01-22T07:04:14.897Z http_only http://backend.fiservis. http://backend.fiservis. n/a - 2019-01-22T07:04:14.897Z http_only http://ap.fiservis.com/ http://ap.fiservis.com/ http://ap.fiservis.com/ n/a - 2019-01-22T07:04:14.897Z http_only http://ap.fiservis.com/ http://ap.fiservis.com/ n/a - 2019-01-22T07:04:14.897Z	http_only	http://ca.fiservls.com/	http://ca.fiservls.com/	n/a	-	
http_only	http_only		http://blog.fiservls.com /	n/a	-	
http_only http://bf.fiservls.com/ http://bf.fiservls.com/ n/a - 2019-01- 22T07:04:16.646Z http_only http://www.fiservls.com/ http://www.fiservls.com/ n/a - 2019-01- 22T07:04:14.897Z http_only http://download.fiservl http://download.fiservl s.com/ s.com/ n/a - 2019-01- 22T07:04:14.897Z http_only http://ns1.fiservls.com/ http://ns1.fiservls.com/ n/a - 2019-01- 22T07:04:14.897Z http_only http://ap.fiservls.com/ http://ap.fiservls.com/ n/a - 2019-01- 22T07:04:14.897Z http_only http://ap.fiservls.com/ http://ap.fiservls.com/ n/a - 2019-01- 22T07:04:14.897Z http_only http://ap.fiservls.com/ http://ap.fiservls.com/ n/a - 2019-01- 22T07:04:14.897Z http_only http://backend.fiservls com/ com/ 2019-01- 22T07:04:14.878Z	http_only	http://bg.fiservls.com/	http://bg.fiservls.com/	n/a	-	
http_only http://ww.fiservls.com/ http://ww.fiservls.com/ n/a - 2019-01-22T07:04:14.897Z http_only http://download.fiservl s.com/ n/a - 2019-01-22T07:04:14.897Z http_only http://ns1.fiservls.com/ http://ns1.fiservls.com/ n/a - 2019-01-22T07:04:14.897Z http_only http://ns1.fiservls.com/ http://ns1.fiservls.com/ n/a - 2019-01-22T07:04:14.897Z http_only http://ap.fiservls.com/ http://ap.fiservls.com/ n/a - 2019-01-22T07:04:14.897Z http_only http://backend.fiservls com/ n/a - 2019-01-22T07:04:14.897Z http_only http://backend.fiservls com/ n/a - 2019-01-22T07:04:14.897Z http_only http://backend.fiservls com/	http_only		· ·	n/a	-	
http_only	http_only	http://bf.fiservls.com/	http://bf.fiservls.com/	n/a	-	
s.com/ s.com/ s.com/ 22T07:04:14.897Z http_only http://ns1.fiservls.com/ http://ns1.fiservls.com/ n/a - 2019-01- 22T07:04:14.897Z http_only http://ap.fiservls.com/ http://ap.fiservls.com/ n/a - 2019-01- 22T07:04:14.897Z http_only http://backend.fiservls http://backend.fiservls. n/a - 2019-01- 22T07:04:14.878Z	http_only	http://ww.fiservls.com/	http://ww.fiservls.com/	n/a	-	
http_only	http_only	•	•	n/a	-	
http_only	http_only	http://ns1.fiservls.com/	http://ns1.fiservls.com/	n/a	-	
.com/ com/ 22T07:04:14.878Z	http_only	http://ap.fiservls.com/	http://ap.fiservls.com/	n/a	-	
http_only http://in.fiservls.com/ http://in.fiservls.com/ n/a - 2019-01-	http_only	•	· ·	n/a	-	
	http_only	http://in.fiservls.com/	http://in.fiservls.com/	n/a	-	2019-01-

					22T07:04:14.878Z
http_only	http://espanol.fiservls.com/	http://espanol.fiservls. com/	n/a	-	2019-01- 22T07:04:14.863Z
http_only	http://forums.fiservls.c om/	http://forums.fiservls.c om/	n/a	-	2019-01- 22T07:04:14.853Z
http_only	http://arizona.fiservls.c om/	http://arizona.fiservls.c om/	n/a	-	2019-01- 22T07:04:14.849Z
http_only	http://chat.fiservls.co m/	http://chat.fiservls.com /	n/a	-	2019-01- 22T07:04:14.849Z
http_only	http://mobile.fiservls.c om/	http://mobile.fiservls.c om/	n/a	-	2019-01- 22T07:04:14.017Z
http_only	http://14.fiservls.com/	http://14.fiservls.com/	n/a	-	2019-01- 22T07:04:14.016Z
http_only	http://boston.fiservls.c om/	http://boston.fiservls.c om/	n/a	-	2019-01- 22T07:04:14.015Z
http_only	http://sadmin.fiservls.c om/	http://sadmin.fiservls.c om/	n/a	-	2019-01- 22T07:04:14.014Z
http_only	http://developer.fiserv ls.com/	http://developer.fiservl s.com/	n/a	-	2019-01- 22T07:04:13.993Z
http_only	http://act.fiservls.com/	http://act.fiservls.com/	n/a	-	2019-01- 22T07:04:13.993Z
http_only	http://client.fiservls.co m/	http://client.fiservls.co m/	n/a	-	2019-01- 22T07:04:13.990Z
http_only	http://backup.fiservls.c om/	http://backup.fiservls.c om/	n/a	-	2019-01- 22T07:04:13.984Z
http_only	http://ftp.fiservls.com/	http://ftp.fiservls.com/	n/a	-	2019-01- 22T07:04:13.780Z
http_only	http://citrix.fiservls.co m/	http://citrix.fiservls.co m/	n/a	-	2019-01- 22T07:04:13.145Z
http_only	http://biz.fiservls.com/	http://biz.fiservls.com/	n/a	-	2019-01- 22T07:04:13.145Z
http_only	http://blackberry.fiserv ls.com/	http://blackberry.fiserv ls.com/	n/a	-	2019-01- 22T07:04:13.145Z
http_only	http://arkansas.fiservls .com/	http://arkansas.fiservls .com/	n/a	-	2019-01- 22T07:04:13.145Z
http_only	http://demo.fiservls.co m/	http://demo.fiservls.co m/	n/a	-	2019-01- 22T07:04:12.815Z
http_only	http://survey.fiservls.c om/	http://survey.fiservls.c om/	n/a	-	2019-01- 22T07:04:12.815Z
http_only	http://arlington.fiservls .com/	http://arlington.fiservls. com/	n/a	-	2019-01- 22T07:04:05.405Z
http_only	http://fiservdox.com/	http://fiservdox.com/	n/a	-	2019-01- 22T07:04:03.821Z

http_only	http://mail.fiservls.com /	http://mail.fiservls.com /	n/a	-	2019-01- 22T07:04:03.030Z
http_only	http://team.fiservls.co m/	http://team.fiservls.co m/	n/a	-	2019-01- 22T07:04:03.013Z
http_only	http://ac.fiservls.com/	http://ac.fiservls.com/	n/a	-	2019-01- 22T07:04:02.968Z
http_only	http://pop.fiservls.com /	http://pop.fiservls.com /	n/a	-	2019-01- 22T07:04:02.920Z
http_only	http://131.fiservls.com/	http://131.fiservls.com/	n/a	-	2019-01- 22T07:04:02.897Z
http_only	http://corp.fiservls.co m/	http://corp.fiservls.com /	n/a	-	2019-01- 22T07:04:02.819Z
http_only	http://apps.fiservls.co m/	http://apps.fiservls.co m/	n/a	-	2019-01- 22T07:04:02.789Z
http_only	http://atlanta.fiservls.c om/	http://atlanta.fiservls.c om/	n/a	-	2019-01- 22T07:04:02.748Z
http_only	http://customer.fiservl s.com/	http://customer.fiservls .com/	n/a	-	2019-01- 22T07:04:02.710Z
http_only	http://intranet1.fiservls.com/	http://intranet1.fiservls.com/	n/a	-	2019-01- 22T07:04:02.673Z
http_only	http://18.fiservls.com/	http://18.fiservls.com/	n/a	-	2019-01- 22T07:04:02.638Z
http_only	http://administrador.fis ervls.com/	http://administrador.fis ervls.com/	n/a	-	2019-01- 22T07:04:02.606Z
http_only	http://apollo.fiservls.c om/	http://apollo.fiservls.co m/	n/a	-	2019-01- 22T07:04:02.487Z
http_only	http://manage.fiservls.com/	http://manage.fiservls. com/	n/a	-	2019-01- 22T07:04:02.415Z
http_only	http://au.fiservls.com/	http://au.fiservls.com/	n/a	-	2019-01- 22T07:04:02.382Z
http_only	http://support.fiservls.com/	http://support.fiservls.c om/	n/a	-	2019-01- 22T07:04:02.382Z
http_only	http://email.fiservls.co m/	http://email.fiservls.co m/	n/a	-	2019-01- 22T07:04:02.030Z
http_only	http://ad.fiservls.com/	http://ad.fiservls.com/	n/a	-	2019-01- 22T07:04:01.957Z
http_only	http://am.fiservls.com/	http://am.fiservls.com/	n/a	-	2019-01- 22T07:04:01.824Z
http_only	http://antivirus.fiservls. com/	http://antivirus.fiservls.com/	n/a	-	2019-01- 22T07:04:01.560Z
http_only	http://california.fiservls .com/	http://california.fiservls .com/	n/a	-	2019-01- 22T07:04:01.560Z
http_only	http://ajax.fiservls.com	http://ajax.fiservls.com	n/a	-	2019-01-

/ / 22T07:04:01.560Z

RECOMMENDATION

Any site served to a user (possibly at the end of a redirect chain) should be served over HTTPS.

ABOUT THIS ISSUE

The site responds to HTTP requests without ultimately redirecting the browser to a secure version of the page. Since the site allows plaintext traffic, a man-in-the-middle attacker is able to read and modify any information passed between the site and the user. There are a variety of situations in which an attacker can intercept plaintext traffic in a man-in-the-middle position, including but not limited to: * Open Wi-Fi Hotspots * WPA/WPA2 encrypted hot-spots where the attacker connected before the victim * Malicious Wi-Fi access points * Compromised switches and routers * ARP poisoning on the same wired network It's important to remember that in many of the above situations, an attacker can not only read traffic, but also actively modify the traffic. Even if a site that does not contain sensitive information, an attacker can still inject malicious content to a user's browser.

APPLICATION SECURITY > ISSUE DETAIL

Insecure HTTPS Redirect Pattern

Site redirects to a domain in a way that limits the security provided by HTTPS and HTTP Strict Transport Security (HSTS) headers; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the site.

-0.9 SCORE

6 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
https_redirect_differe nt_apex	https://fiserv.service-now.com/auth_redire ct.do? sysparm_url=https%3 a%2f%2flogin.microso ftonline.com%2fte%2ff iservservicepoint.onm icrosoft.com%2fb2c_1 a_prod_sn_signin%2f samlp%2fsso%2flogin %3fsamlrequest%3dlvl bbptaep0vthdgoxfjvs yssvxvupki2o2hf2sdg 7mszjcdhsr%252fx8a kts%252bwep15896b n7ni3drxq7lopeedphf aznttamr17qsis6his2gf ugfwrld77o5wxyfursv hbdxcy5jboko4iesuab sh25scfj7cpuljuzzvgfz mapubn1s%252b0ktq uboi7lt9gqak4w0haw b1ypr3rqatwaaxhswm yhhwbmeadtctzpwtgx qb4qd2qt3em2ouhxnl	http://my.carreker.com	http://my.carreker.com /, 302, https://c3.fiserv.com/, 302, https://servicepoint.fis ervapps.com/, 302, https://fiserv.servicenow.com/, 302, https://fiserv.servicenow.com/, 302, https://fiserv.servicenow.com/auth_redirect.do? sysparm_url=https%3 A%2F%2Flogin.microsoftonline.com%2Fte% 2Ffiservservicepoint.onmicrosoft.com%2F82 C_1A_Prod_sn_signin %2Fsamlp%2Fsso%2F login%3FSAMLRequest%3DIVLBbptAEPOVtHdgoXFjVsYSsVXVUpKi2O2hF2sDg7MSzJCdhSR%252FX8AkTS%2 52BWep15896bN7Ni3dRxq7LOPeEDPHfAzn	Redirect goes to different apex domain	2019-01- 29T09:11:00.692Z

	5zhvvoachenvutzkoia		ttamD17gSic6blc2GEu		
	5zhxyoaebsnxwtzkpjo %252f8l6rlwbkihwvrh met9umyn%252b%25 2fwzz6uutfnxyvchlhe qrf4ssyizfy%252buqx quqa5fwzmx5s4ww3tj j3sen2gl0qyhklvoz8o dnirewrkjk4sulfwsvnc g8mlgzpl%252fn%25 2bpinyft8ccj%252f%2 52fst9mbl0pwd4p6p %252bk%252bhdynm iemmv6nd1btbt5xe4 7ei%252f312sl0uvws8 cs1yrrte7bu61kd68rk7 pzwnbu48yh5s02l32 mfzm6vctvlxjwuwanqj xs%252bq%252fd77% 252baw%253d%253d %26relaystate%3dhttp s%253a%252f%252ffi serv.service- now.com%252fnavpa ge.do		ttamR17qSis6hls2GFu gFWrlD77O5WxYFUrS VHBdXCy5jBOkO4leS uAbsH25sCfj7cpuLJu ZZVGFZmAPUBn1s%2 52B0ktQUBOi7lt9gqA k4W0HAwb1yPR3rqaT waAxhSWmyhHWBmE adTCTzpwtGXQB4Qd 2Qt3Em2OUHXNL5Z HxyOaEBsNxwTZkpjO %252F8L6RLWBKIhW VrhmEt9umYn%252B %252FWZZ6UUTFNX yVchlHEqrF4ssyiZfy% 252BuqxquQA5Fwzm x5S4Ww3TjJ3sEN2Gl OqYhklvoz8ODnlREW RkjK4SuLfwsvnCG8Ml gZPl%252FN%252BPl NYfT8ccj%252FN%252BPl NYfT8ccj%252FN%253DW258Pl NyfT8ccj%253DW258Pl NyfT8ccj%253DW258Pl NyfT8ccj%253DW258Pl NyfT8ccj%253DW258Pl NyfT8ccj%253DW258Pl NyfT8ccj%252FN%253DW258Pl NyfT8ccj%252FN%253DW258Pl NyfT8ccj%252FN%253DW258Pl NyfT8ccj%253DW258Pl NyfT8ccj%252Pl NyfT8ccj%252P		
https_redirect_differe nt_apex	https://www.fiserv.co m/index.aspx	http://www.summitsite.com/	http://www.summitsite. com/, 301, https://www.fiserv.com , 301, https://www.fiserv.com /index.aspx	Redirect goes to different apex domain	2019-01- 29T09:10:54.588Z
Evidence: Strict-Transport-Security: m	nax-age=31536000				
https_redirect_differe nt_apex	https://auth01.client-central.com/nidp/idff/s so? requestid=idjrjdyv6vz onct0nte5k88oirdqi& majorversion=1&minor version=2&issueinsta nt=2019-01-29t09%3a10%3a52z& providerid=https%3a%2f%2fwww.client-central.com%3a443%2fnesp%2fidff%2fmet adata&relaystate=ma%3d%3d&consent=urn%3aliberty%3aconsent%3aunavailable&agappna=clientcentral_home&forceauthn=false&ispassive=false&na	http://www.fiserveft.com/	http://www.fiserveft.co m/, 302, https://www.client-central.com/, 302, https://www.client-central.com:443/nesp/app/plogin? agAppNa=clientCentral_Home&c=radius/to ken/uri⌖=%22htt ps://www.client-central.com/%22, 302, https://auth01.client-central.com/nidp/idff/s so? RequestID=idJrJDYV6 VZoncTOnte5K88OIR dql&MajorVersion=1& MinorVersion=2&Issue Instant=2019-01-	Redirect goes to different apex domain	2019-01- 29T09:10:53.040Z

	meidpolicy=onetime& protocolprofile=http% 3a%2f%2fprojectlibert y.org%2fprofiles%2fbr ws-art⌖=https%3a% 2f%2fwww.client-central.com%2f&auth ncontextstatementref =radius%2ftoken%2fur i		29T09%3A10%3A52Z &ProviderID=https%3A %2F%2Fwww.client- central.com%3A443% 2Fnesp%2Fidff%2Fme tadata&RelayState=M A%3D%3D&consent=u rn%3Aliberty%3Acons ent%3Aunavailable&a gAppNa=clientCentral _Home&ForceAuthn=f alse&IsPassive=false& NameIDPolicy=onetim e&ProtocolProfile=http %3A%2F%2Fprojectlib erty.org%2Fprofiles%2 Fbrws- art⌖=https%3A% 2F%2Fwww.client- central.com%2F&Auth nContextStatementRe f=radius%2Ftoken%2F uri		
Evidence: Strict-Transport-Security: m	nax-age=31536000;includeSu	bDomains			
https_redirect_add_s ubdomain	https://www.fiservweb solutions.com	http://fiservwebsolutio ns.com/	http://fiservwebsolutio ns.com/, 301, https://www.fiservweb solutions.com	Redirect goes to a different subdomain	2019-01- 29T09:10:52.406Z
https_redirect_add_s ubdomain	https://www.fiserv.co m/index.aspx	http://fiserv.com/	http://fiserv.com/, 302, https://www.fiserv.com /, 301, https://www.fiserv.com /index.aspx	Redirect goes to a different subdomain	2019-01- 29T09:09:40.297Z
Evidence: Strict-Transport-Security: m	nax-age=31536000				
https_redirect_hsts_h eader_missing_includ esubdomains	https://www.fiserv.co m/index.aspx	http://test.fiserv.com/	http://test.fiserv.com/, 301, https://www.fiserv.com , 301, https://www.fiserv.com /index.aspx	HSTS header missing includeSubDomains directive	2019-01- 29T09:09:29.254Z
Evidence: Strict-Transport-Security: m	nax-age=31536000				

RECOMMENDATION

Any HTTP site should redirect the user to a secure (i.e. HTTPS) version of the same domain that was originally requested (or a higher-level/parent version of that same domain). For example, http://www.example.com should only redirect either to https://www.example.com or https://example.com. This redirect should be done before redirecting to any other domain or subdomain.

ABOUT THIS ISSUE

The HTTP site redirects users to a new URL in a way that cannot be secured with HTTPS and HSTS headers. This leaves users open to man-in-the-middle attackers who can redirect them to a fraudulent/ spoofed version of the intended site. Please see "Site Does Not Enforce HTTPS" issue type for more information regarding man-in-the-middle scenarios.

APPLICATION SECURITY > ISSUE DETAIL

Redirect Chain Contains HTTP

Site redirects through URLs that are not secured with HTTPS; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the intended destination site.

-0.9 SCORE

4 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
redirect_chain_contai ns_http	https://www.fiserv.co m/industries/credit- unions/account- processing- platforms/galaxy.aspx	http://www.fiserv- galaxy.com/	http://www.fiserv-galaxy.com/, 302, http://www.fiserv.com/ industries/credit- unions/account- processing- platforms/galaxy.aspx, 302, https://www.fiserv.com/ industries/credit- unions/account- processing- platforms/galaxy.aspx	Redirect chain contains an HTTP destination	2019-01- 29T09:10:53.696Z
redirect_chain_contai ns_http	https://www.fiserv- ecomhosting.com/log on.asp	http://www.fiserv- ecomhosting.com/	http://www.fiserv- ecomhosting.com/, 302, http://www.fiserv- ecomhosting.com/log on.asp, 302, https://www.fiserv- ecomhosting.com/log on.asp	Redirect chain contains an HTTP destination	2019-01- 29T09:10:53.649Z
redirect_chain_contai ns_http	https://www.careers.fi serv.com/	https://careers.fiserv.c om/	https://careers.fiserv.c om/, 301, http://www.careers.fis erv.com, 301, https://www.careers.fi serv.com/	Redirect chain contains an HTTP destination	2019-01- 29T09:09:27.681Z
redirect_chain_contai ns_http	https://fiservsupport.c om/	http://www.fiservsupp ort.com/	http://www.fiservsupp ort.com/, 302, http://fiservsupport.co m/, 302, https://fiservsupport.c om/	Redirect chain contains an HTTP destination	2019-01- 22T07:04:04.073Z

RECOMMENDATION

Any HTTP site should immediately redirect users to HTTPSprotected URLs and ensure that any further redirects do not occur over HTTP. Prefer the usage of HTTPS URLs over HTTP when available, avoiding an unnecessary redirect.

ABOUT THIS ISSUE

While redirecting a user to their ultimate URL destination, the user passes through one or more URLs served over HTTP (instead of HTTPS). Having HTTP links in a redirect chain weakens other security technologies (e.g., HTTPS and HSTS headers) that are deployed elsewhere in the chain.

APPLICATION SECURITY > ISSUE DETAIL

1 Unsafe Implementation Of Subresource Integrity

Subresource integrity (SRI) is a security feature that enables browsers to verify that files they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing website elements to provide a cryptographic hash that a fetched file must match.

7 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
ri_not_implemented	http://agility- fiserv.com/	http://agility- fiserv.com/	n/a	-	2019-01- 29T09:10:55.566Z
ividence: script src="https://www.sc ype="text/javascript">	.pages05.net/lp/static/js/iMA\	WebCookie.js?3859023a-142	e3c17146-c6f842ded9e6d11c5ff	ebd715e129037&h=www.pa	ages05.net"
ri_not_implemented	http://bbs.summitsite. com/	http://bbs.summitsite.c om/	n/a	-	2019-01- 29T09:10:53.790Z
ividence: /script src="https://www.sc /ype="text/javascript">	.pages05.net/lp/static/js/iMA\	WebCookie.js?3859023a-142	e3c17146-c6f842ded9e6d11c5ff	ebd715e129037&h=www.pa	ages05.net"
ri_not_implemented	https://www.fiserv.co m/industries/credit- unions/account- processing- platforms/galaxy.aspx	https://www.fiserv-galaxy.com/	https://www.fiserv- galaxy.com/, 302, http://www.fiserv.com/ industries/credit- unions/account- processing- platforms/galaxy.aspx, 302, https://www.fiserv.com /industries/credit- unions/account- processing- platforms/galaxy.aspx	-	2019-01- 29T09:10:53.771Z
			e3c17146-c6f842ded9e6d11c5ff his_widget.js#pubid=ra-58beb6		ages05.net"
ri_not_implemented	https://www.fiservdox.com/	https://www.fiservdox. com/	n/a	-	2019-01- 29T09:10:53.470Z
ividence: script src="https://www.sc ype="text/javascript">	.pages05.net/lp/static/js/iMA\	WebCookie.js?3859023a-142	e3c17146-c6f842ded9e6d11c5ff	ebd715e129037&h=www.pa	ages05.net"
ri_not_implemented	http://www.fiservdox.c om/	http://www.fiservdox.c om/	n/a	-	2019-01- 29T09:10:53.412Z
ividence: /script src="https://www.sc /ype="text/javascript">	.pages05.net/lp/static/js/iMA\	WebCookie.js?3859023a-142	e3c17146-c6f842ded9e6d11c5ff	ebd715e129037&h=www.pa	ages05.net"
ri_not_implemented	https://www.fiservweb solutions.com	http://fiservwebsolutio ns.com/	http://fiservwebsolutio ns.com/, 301, https://www.fiservweb solutions.com	-	2019-01- 29T09:10:52.406Z

Evidence:

link rel='stylesheet' id='google-fonts-css' href='//fonts.googleapis.com/css?

family=Open+Sans%3A400%2C400italic%2C300%2C600%2C600%2C600%2C600talic%7CLato%3A400%2C100%2C300%2C700%7CJosefin+Slab%3A400%2C100%2C100italic%2C300%2C300italic%2C400italic%2C400italic%2C400italic%2C400italic%2C400italic%2C400italic%2C400italic%2C400italic%2C400italic%2C400italic%2C400italic%2C400italic%2C400italic%2C400italic%2C400italic%2C500%2C500italic%2C700italic%2C700%2C900%2C900italic%2C700italic%2C700italic%2C700italic%2C700%2C900italic%2C400italic%2C500%2C900italic%2C700%2C900italic%2C700%2C900italic%2C500%2C900italic%2C700%2C900italic%2C900%2C900italic%2C700%2C900italic%2C900%2C900italic%2C900itali

sri_not_implemented	https://www.careers.fi serv.com/	https://careers.fiserv.c om/	https://careers.fiserv.c om/, 301, http://www.careers.fis erv.com, 301, https://www.careers.fi serv.com/	-	2019-01- 29T09:09:27.681Z
---------------------	-------------------------------------	---------------------------------	---	---	------------------------------

Evidence:

< link rel="stylesheet" type="text/css" href="//tbcdn.talentbrew.com/company/1758/v1/js/slick.css"/>,<link rel="stylesheet" href="/tbcdn.talentbrew.com/company/1758/css/4471-Full.css"/>,<link rel="stylesheet" type="text/css" href="http://localhost/fiserv/company/tb/css/style.css">,<script src="//tbcdn.talentbrew.com/js/client/adframe.js">,<script src="//players.brightcove.net/2474524878001/default_default/index.min.js">,<script src="//tbcdn.talentbrew.com/bundles/tb-core">,<script src="//tbcdn.talentbrew.com/bundles/tb-core">,<script src="//tbcdn.talentbrew.com/company/1758/v1/js/slick.min.js">,<script src="//use.fontawesome.com/bb4a8a1a47.js">,<script src="//tbcdn.talentbrew.com/company/1758/js/4471-Full.min.js">,<script src="//tbcdn.talentbrew.com/bundles/form">,<script id="tmp-magic-bullet" src="/tbcdn.talentbrew.com/company/1758/js/4471-Full.min.js">,<script src="/tbcdn.talentbrew.com/bundles/form">,<script id="tmp-magic-bullet" src="https://services.tmpwebeng.com/magicbullet/" data-gdpr="true" data-gdpr-policy-url="https://www.fiserv.com/about/privacypolicy.aspx" data-gdpr-client-name="fisery">

RECOMMENDATION

Please ensure that all website elements (i.e. <script> and <link>) loading JavaScript and CSS stylesheets hosted with external organizations contain the 'integrity' directive with a valid checksum. Example: <script src="https://example.com/example-framework.js" integrity="sha384-

oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQIGYI1kPz Qho1wx4JwY8wC" crossorigin="anonymous"></script>

ABOUT THIS ISSUE

Many websites that rely on JavaScript and CSS stylesheet files will host these static resources with external organizations (typically CDNs) to improve website load times. Unfortunately, if one of these external organizations is compromised then the JavaScript and CSS files it hosts can also be compromised and used to push malicious code to the original website. Subresource integrity is a way for a website owner to add a checksum value to all externally-hosted files that is used by the browser to verify that files loaded from external organizations have not been modified.

APPLICATION SECURITY > ISSUE DETAIL

Website does not implement X-Frame-Options Best Practices

Not explicitly setting X-Frame-Options allows other, untrusted, websites to embed your site in a frame on their page. This can be used to make social engineering attacks appear more legitimate, or can even be used for clickjacking attacks.

-0.9 SCORE

143 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
x_frame_options_mis sing	https://staging.fiserv- ecomhosting.com/	https://staging.fiserv- ecomhosting.com/	n/a	Header missing	2019-01- 29T09:11:43.731Z
x_frame_options_mis sing	http://staging.fiserv- ecomhosting.com/	http://staging.fiserv- ecomhosting.com/	n/a	Header missing	2019-01- 29T09:11:43.673Z
x_frame_options_mis sing	http://www.fiservsw.c om/	http://www.fiservsw.co m/	n/a	Header missing	2019-01- 29T09:11:42.823Z
x_frame_options_mis sing	https://mail.fiservlendi ngsolutions.com/	https://mail.fiservlendi ngsolutions.com/	n/a	Header missing	2019-01- 29T09:11:17.099Z

x_frame_options_mis sing	http://fiservcreditservices.com/	http://fiservcreditservices.com/	n/a	Header missing	2019-01- 29T09:11:15.569Z
x_frame_options_mis sing	https://webmail.fiserv. net/	https://webmail.fiserv. net/	n/a	Header missing	2019-01- 29T09:11:13.849Z
x_frame_options_mis sing	http://fiservsw.com/	http://fiservsw.com/	n/a	Header missing	2019-01- 29T09:11:05.384Z
x_frame_options_mis sing	https://my.carreker.co m/login.asp	https://my.carreker.co m/	https://my.carreker.co m/, 302, https://my.carreker.co m/Login.asp	Header missing	2019-01- 29T09:10:59.822Z
x_frame_options_mis sing	https://search.carreke r.com/	https://search.carreker .com/	n/a	Header missing	2019-01- 29T09:10:57.094Z
x_frame_options_mis sing	http://search.carreker. com/	http://search.carreker. com/	n/a	Header missing	2019-01- 29T09:10:57.065Z
x_frame_options_mis sing	https://careers.carrek er.com/	https://careers.carreke r.com/	n/a	Header missing	2019-01- 29T09:10:56.934Z
x_frame_options_mis sing	https://mail.billmatrix.c om/	https://mail.billmatrix.c om/	n/a	Header missing	2019-01- 29T09:10:56.928Z
x_frame_options_mis sing	http://careers.carreker .com/	http://careers.carreker .com/	n/a	Header missing	2019-01- 29T09:10:56.855Z
x_frame_options_mul tiple	https://fiservdm.net/vp n/index.html	https://fiservdm.net/	https://fiservdm.net/, 302, https://fiservdm.net/vp n/index.html	Multiple headers found	2019-01- 29T09:10:55.671Z
Evidence: X-Frame-Options: SAMEOR	RIGIN,X-Frame-Options: SAME	EORIGIN			
x_frame_options_mis sing	https://support.fiservat lanta.net/	http://support.fiservatl anta.net/	http://support.fiservatl anta.net/, 302, https://support.fiservat lanta.net/	Header missing	2019-01- 29T09:10:54.014Z
x_frame_options_mis sing	https://fiserv- ecomhosting.com/log on.asp	https://fiserv- ecomhosting.com/	https://fiserv- ecomhosting.com/, 302, https://fiserv- ecomhosting.com/log on.asp	Header missing	2019-01- 29T09:10:53.901Z
x_frame_options_mis sing	https://fiservwebsoluti ons.com/	https://fiservwebsoluti ons.com/	n/a	Header missing	2019-01- 29T09:10:53.876Z
x_frame_options_mis sing	https://www.fiserv- ecomhosting.com/log on.asp	http://www.fiserv- ecomhosting.com/	http://www.fiserv- ecomhosting.com/, 302, http://www.fiserv- ecomhosting.com/log on.asp, 302, https://www.fiserv- ecomhosting.com/log on.asp	Header missing	2019-01- 29T09:10:53.649Z
x_frame_options_mis sing	https://alpha.hepsiian. com/	https://alpha.hepsiian. com/	n/a	Header missing	2019-01- 29T09:10:53.348Z
x_frame_options_mis sing	https://images.hepsiia n.com/	https://images.hepsiia n.com/	n/a	Header missing	2019-01- 29T09:10:52.534Z

x_frame_options_mis sing	https://fiservsupport.c om/	http://fiservsupport.co m/	http://fiservsupport.co m/, 302, https://fiservsupport.c om/	Header missing	2019-01- 29T09:10:51.744Z
x_frame_options_mis sing	https://fiservlendingso lutions.com/	https://fiservlendingsol utions.com/	n/a	Header missing	2019-01- 29T09:10:50.983Z
x_frame_options_mis sing	http://fiservlendingsol utions.com/	http://fiservlendingsol utions.com/	n/a	Header missing	2019-01- 29T09:10:50.913Z
x_frame_options_mis sing	https://fiservipvpn.co m/	https://fiservipvpn.com /	n/a	Header missing	2019-01- 29T09:10:50.584Z
x_frame_options_mis sing	http://demo.billmatrix. com/	http://demo.billmatrix. com/	n/a	Header missing	2019-01- 29T09:10:50.447Z
x_frame_options_mis sing	https://www.fiservlend ingsolutions.com/	https://www.fiservlend ingsolutions.com/	n/a	Header missing	2019-01- 29T09:10:50.369Z
x_frame_options_mis sing	http://mail.fiservlendin gsolutions.com/	http://mail.fiservlendin gsolutions.com/	n/a	Header missing	2019-01- 29T09:10:50.349Z
x_frame_options_mis sing	http://www.fiservlendi ngsolutions.com/	http://www.fiservlendi ngsolutions.com/	n/a	Header missing	2019-01- 29T09:10:50.285Z
x_frame_options_mis sing	https://fiservcws.com/	https://fiservcws.com/	n/a	Header missing	2019-01- 29T09:10:50.069Z
x_frame_options_mul tiple	https://fiservdmdr.net/ vpn/index.html	https://fiservdmdr.net/	https://fiservdmdr.net/, 302, https://fiservdmdr.net/ vpn/index.html	Multiple headers found	2019-01- 29T09:10:49.321Z
Evidence: X-Frame-Options: SAMEOR	RIGIN,X-Frame-Options: SAMI	EORIGIN			
x_frame_options_mis sing	https://www.careers.fi serv.com/	https://careers.fiserv.c om/	https://careers.fiserv.c om/, 301, http://www.careers.fis erv.com, 301, https://www.careers.fi serv.com/	Header missing	2019-01- 29T09:09:27.681Z
x_frame_options_mis sing	https://alabama.fiservl s.com/	https://alabama.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:16.824Z
x_frame_options_mis sing	http://alabama.fiservls. com/	http://alabama.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:16.763Z
x_frame_options_mis sing	https://en.fiservls.com /	https://en.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:16.760Z
x_frame_options_mis sing	https://blog.fiservls.co m/	https://blog.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:16.759Z
x_frame_options_mis sing	https://ca.fiservls.com/	https://ca.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:16.742Z
x_frame_options_mis sing	https://shop.fiservls.co m/	https://shop.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:16.731Z
x_frame_options_mis sing	https://bg.fiservls.com /	https://bg.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:16.726Z

x_frame_options_mis sing	https://bf.fiservls.com/	https://bf.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:16.715Z
x_frame_options_mis sing	http://ca.fiservls.com/	http://ca.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:16.691Z
x_frame_options_mis sing	http://en.fiservls.com/	http://en.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:16.691Z
x_frame_options_mis sing	http://blog.fiservls.co m/	http://blog.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:16.677Z
x_frame_options_mis sing	http://shop.fiservls.co m/	http://shop.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:16.662Z
x_frame_options_mis sing	http://bg.fiservls.com/	http://bg.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:16.662Z
x_frame_options_mis sing	http://bf.fiservls.com/	http://bf.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:16.646Z
x_frame_options_mis sing	https://ap.fiservls.com/	https://ap.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.968Z
x_frame_options_mis sing	https://in.fiservls.com/	https://in.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.961Z
x_frame_options_mis sing	https://ww.fiservls.co m/	https://ww.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:14.955Z
x_frame_options_mis sing	https://chat.fiservls.co m/	https://chat.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:14.953Z
x_frame_options_mis sing	https://backend.fiservl s.com/	https://backend.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:14.953Z
x_frame_options_mis sing	https://espanol.fiservls .com/	https://espanol.fiservls .com/	n/a	Header missing	2019-01- 22T07:04:14.953Z
x_frame_options_mis sing	https://arizona.fiservls. com/	https://arizona.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:14.918Z
x_frame_options_mis sing	http://ap.fiservls.com/	http://ap.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.897Z
x_frame_options_mis sing	http://ns1.fiservls.com/	http://ns1.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.897Z
x_frame_options_mis sing	http://download.fiservl s.com/	http://download.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:14.897Z
x_frame_options_mis sing	http://ww.fiservls.com/	http://ww.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.897Z
x_frame_options_mis sing	http://backend.fiservls .com/	http://backend.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:14.878Z
x_frame_options_mis sing	http://in.fiservls.com/	http://in.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.878Z
x_frame_options_mis sing	http://espanol.fiservls. com/	http://espanol.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:14.863Z
x_frame_options_mis sing	http://forums.fiservls.c om/	http://forums.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:14.853Z

x_frame_options_mis sing	http://arizona.fiservls.c om/	http://arizona.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:14.849Z
x_frame_options_mis sing	http://chat.fiservls.co m/	http://chat.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:14.849Z
x_frame_options_mis sing	https://14.fiservls.com/	https://14.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.091Z
x_frame_options_mis sing	https://mobile.fiservls.com/	https://mobile.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.089Z
x_frame_options_mis sing	https://sadmin.fiservls. com/	https://sadmin.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:14.085Z
x_frame_options_mis sing	https://boston.fiservls. com/	https://boston.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:14.083Z
x_frame_options_mis sing	https://developer.fiser vls.com/	https://developer.fiser vls.com/	n/a	Header missing	2019-01- 22T07:04:14.073Z
x_frame_options_mis sing	https://act.fiservls.com /	https://act.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:14.070Z
x_frame_options_mis sing	https://client.fiservls.c om/	https://client.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:14.063Z
x_frame_options_mis sing	https://arlington.fiservl s.com/	https://arlington.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:14.063Z
x_frame_options_mis sing	https://ftp.fiservls.com /	https://ftp.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.047Z
x_frame_options_mis sing	http://mobile.fiservls.c om/	http://mobile.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:14.017Z
x_frame_options_mis sing	http://14.fiservls.com/	http://14.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:14.016Z
x_frame_options_mis sing	http://boston.fiservls.c om/	http://boston.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:14.015Z
x_frame_options_mis sing	http://sadmin.fiservls.c om/	http://sadmin.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:14.014Z
x_frame_options_mis sing	http://developer.fiserv ls.com/	http://developer.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:13.993Z
x_frame_options_mis sing	http://act.fiservls.com/	http://act.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:13.993Z
x_frame_options_mis sing	http://client.fiservls.co m/	http://client.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:13.990Z
x_frame_options_mis sing	http://backup.fiservls.c om/	http://backup.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:13.984Z
x_frame_options_mis sing	http://ftp.fiservls.com/	http://ftp.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:13.780Z
x_frame_options_mis sing	https://blackberry.fiser vls.com/	https://blackberry.fiser vls.com/	n/a	Header missing	2019-01- 22T07:04:13.296Z
x_frame_options_mis	https://citrix.fiservls.co	https://citrix.fiservls.co	n/a	Header missing	2019-01-

sing	m/	m/			22T07:04:13.214Z
x_frame_options_mis sing	https://arkansas.fiservl s.com/	https://arkansas.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:13.209Z
x_frame_options_mis sing	https://biz.fiservls.com /	https://biz.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:13.207Z
x_frame_options_mis sing	http://citrix.fiservls.co m/	http://citrix.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:13.145Z
x_frame_options_mis sing	http://blackberry.fiserv ls.com/	http://blackberry.fiserv ls.com/	n/a	Header missing	2019-01- 22T07:04:13.145Z
x_frame_options_mis sing	http://biz.fiservls.com/	http://biz.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:13.145Z
x_frame_options_mis sing	http://arkansas.fiservls .com/	http://arkansas.fiservls .com/	n/a	Header missing	2019-01- 22T07:04:13.145Z
x_frame_options_mis sing	https://demo.fiservls.c om/	https://demo.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:12.891Z
x_frame_options_mis sing	https://survey.fiservls.com/	https://survey.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:12.891Z
x_frame_options_mis sing	https://au.fiservls.com/	https://au.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:12.849Z
x_frame_options_mis sing	http://survey.fiservls.c om/	http://survey.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:12.815Z
x_frame_options_mis sing	http://demo.fiservls.co m/	http://demo.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:12.815Z
x_frame_options_mul tiple	https://flagstar- devicemanager- uat.fiservapps.com/	https://flagstar- devicemanager- uat.fiservapps.com/	n/a	Multiple headers found	2019-01- 22T07:04:09.273Z
Evidence: X-Frame-Options: DENY,X-	Frame-Options: sameorigin				
x_frame_options_mis sing	http://arlington.fiservls .com/	http://arlington.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:05.405Z
x_frame_options_mis sing	http://fiservdox.com/	http://fiservdox.com/	n/a	Header missing	2019-01- 22T07:04:03.821Z
x_frame_options_mis sing	https://team.fiservls.co m/	https://team.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:03.075Z
x_frame_options_mis sing	https://ac.fiservls.com/	https://ac.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:03.053Z
x_frame_options_mis sing	http://mail.fiservls.com /	http://mail.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:03.030Z
x_frame_options_mis sing	http://team.fiservls.co m/	http://team.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:03.013Z
x_frame_options_mis sing	https://ns1.fiservls.com /	https://ns1.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:03.005Z
x_frame_options_mis sing	https://131.fiservls.com /	https://131.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:02.976Z

x_frame_options_mis sing	http://ac.fiservls.com/	http://ac.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.968Z
x_frame_options_mis sing	https://forums.fiservls.com/	https://forums.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.940Z
x_frame_options_mis sing	http://pop.fiservls.com /	http://pop.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:02.920Z
x_frame_options_mis sing	https://corp.fiservls.co m/	https://corp.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:02.904Z
x_frame_options_mis sing	http://131.fiservls.com/	http://131.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.897Z
x_frame_options_mis sing	https://apps.fiservls.co m/	https://apps.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:02.857Z
x_frame_options_mis sing	https://atlanta.fiservls. com/	https://atlanta.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:02.851Z
x_frame_options_mis sing	http://corp.fiservls.co m/	http://corp.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:02.819Z
x_frame_options_mis sing	http://apps.fiservls.co m/	http://apps.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:02.789Z
x_frame_options_mis sing	https://customer.fiserv ls.com/	https://customer.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:02.784Z
x_frame_options_mis sing	https://intranet1.fiservl s.com/	https://intranet1.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:02.756Z
x_frame_options_mis sing	http://atlanta.fiservls.c om/	http://atlanta.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:02.748Z
x_frame_options_mis sing	https://18.fiservls.com/	https://18.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.716Z
x_frame_options_mis sing	http://customer.fiservl s.com/	http://customer.fiservls .com/	n/a	Header missing	2019-01- 22T07:04:02.710Z
x_frame_options_mis sing	https://administrador.fi servls.com/	https://administrador.fi servls.com/	n/a	Header missing	2019-01- 22T07:04:02.681Z
x_frame_options_mis sing	http://intranet1.fiservls. com/	http://intranet1.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:02.673Z
x_frame_options_mis sing	http://18.fiservls.com/	http://18.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.638Z
x_frame_options_mis sing	http://administrador.fis ervls.com/	http://administrador.fis ervls.com/	n/a	Header missing	2019-01- 22T07:04:02.606Z
x_frame_options_mis sing	https://backup.fiservls. com/	https://backup.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:02.590Z
x_frame_options_mis sing	https://apollo.fiservls.c om/	https://apollo.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:02.577Z
x_frame_options_mis sing	https://manage.fiservl s.com/	https://manage.fiservls .com/	n/a	Header missing	2019-01- 22T07:04:02.496Z
x_frame_options_mis	http://apollo.fiservls.c	http://apollo.fiservls.co	n/a	Header missing	2019-01-

sing	om/	m/			22T07:04:02.487Z
x_frame_options_mis sing	https://support.fiservls .com/	https://support.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:02.457Z
x_frame_options_mis sing	http://manage.fiservls. com/	http://manage.fiservls. com/	n/a	Header missing	2019-01- 22T07:04:02.415Z
x_frame_options_mis sing	http://support.fiservls.com/	http://support.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:02.382Z
x_frame_options_mis sing	http://au.fiservls.com/	http://au.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.382Z
x_frame_options_mis sing	https://email.fiservls.c om/	https://email.fiservls.c om/	n/a	Header missing	2019-01- 22T07:04:02.113Z
x_frame_options_mis sing	https://ad.fiservls.com /	https://ad.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:02.039Z
x_frame_options_mis sing	http://email.fiservls.co m/	http://email.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:02.030Z
x_frame_options_mis sing	https://download.fiser vls.com/	https://download.fiser vls.com/	n/a	Header missing	2019-01- 22T07:04:02.000Z
x_frame_options_mis sing	http://ad.fiservls.com/	http://ad.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:01.957Z
x_frame_options_mis sing	https://am.fiservls.com /	https://am.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:01.913Z
x_frame_options_mis sing	http://am.fiservls.com/	http://am.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:01.824Z
x_frame_options_mis sing	https://california.fiservl s.com/	https://california.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:01.632Z
x_frame_options_mis sing	https://antivirus.fiservl s.com/	https://antivirus.fiservl s.com/	n/a	Header missing	2019-01- 22T07:04:01.624Z
x_frame_options_mis sing	https://ajax.fiservls.co m/	https://ajax.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:01.621Z
x_frame_options_mis sing	https://pop.fiservls.co m/	https://pop.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:01.617Z
x_frame_options_mis sing	https://mail.fiservls.co m/	https://mail.fiservls.co m/	n/a	Header missing	2019-01- 22T07:04:01.617Z
x_frame_options_mis sing	http://ajax.fiservls.com /	http://ajax.fiservls.com /	n/a	Header missing	2019-01- 22T07:04:01.560Z
x_frame_options_mis sing	http://antivirus.fiservls. com/	http://antivirus.fiservls.com/	n/a	Header missing	2019-01- 22T07:04:01.560Z
x_frame_options_mis sing	http://california.fiservls .com/	http://california.fiservls .com/	n/a	Header missing	2019-01- 22T07:04:01.560Z

RECOMMENDATION

Add one of the following headers, using the 'DENY' or 'ALLOW-FROM' directive, to responses from this website: X-Frame-Options: DENY' X-Frame-Options: ALLOW-FROM https://example.com/'

ABOUT THIS ISSUE

The X-Frame-Options HTTP response header can be used to indicate whether a browser should be allowed to render a page in a '<frame>', '<iframe>' or '<object>'. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other websites.

APPLICATION SECURITY > ISSUE DETAIL



Session Cookie Missing 'HttpOnly' Attribute

Data may be exposed to unauthorized parties during cookie transmission and increases the risk of cross-site scripting (XSS) attacks.

-0.2 SCORE IMPACT

2 findings

HOSTNAME	URL	COOKIE NAME	RAW COOKIE	LAST SEEN
www.fiserv- ecomhosting.com	http://fiserv- ecomhosting.com/	ASPSESSIONID	ASPSESSIONIDCWTATAD B=JPGJJLAAMKBDFLCBBP GBDHNM; secure; path=/	2019-01- 30T00:00:00.000Z
fiserv-ecomhosting.com	https://fiserv- ecomhosting.com/	ASPSESSIONID	ASPSESSIONIDCWTATAD B=LPGJJLAALLENJEIODEA FGJIN; secure; path=/	2019-01- 30T00:00:00.000Z

RECOMMENDATION

Set session cookies with the 'HttpOnly' attribute to ensure they can not be accessed by any other means. A cookie marked with 'HttpOnly' will prevent any malicious injected scripts from being able to access it.

ABOUT THIS ISSUE

The cookie session ID is not set with the 'HttpOnly' attribute. The missing attribute could allow the session ID to be accessed by a client side script such as JavaScript. This exposes the cookies to potential theft via scripting attack vectors, such as XSS attacks.



70 CUBIT SCORE

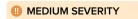
ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

This proprietary module measures a variety of security issues that a company might have. For example, we check public threat intelligence databases for IP addresses that have been flagged. These misconfigurations may have high exploitability and could cause significant harm to the privacy of your data and infrastructure.









Exposed Subdomain



There are no Positive Risk Issues to detect for Cubit Score



3

Possible Typosquat Domains Detected

CUBIT SCORE > ISSUE DETAIL

Exposed Subdomain

An administrative subdomain was detected on public Internet. That subdomain may be vulnerable to unauthorized access.

-1.0 SCORE IMPACT

3 findings

	SUBDOMAIN
admin.fiservcreditservices.com	
intranet.fiserv.com	
intranet.fiservpit.com	

RECOMMENDATION

Resolve all private subdomains using a segregated, internal DNS server. If public exposure is required for these subdomains, it is advised that the integration prevent unauthorized access to the subdomains, either through exploitation or credential compromise. Implementing an IP whitelist for access to internal administrative subdomains would restrict unauthorized access attempts from successfully connecting via the public Internet.

ABOUT THIS ISSUE

A subdomain was detected on target domain names that are accessible to the public Internet. There is a possibility that this subdomain may be a portal to administrative functionalities for various enterprise applications.



100 HACKER CHATTER

ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

The SecurityScorecard Hacker Chatter module is an automated collection and aggregation system for the analysis of multiple streams of underground hacker chatter. Forums, IRC, social networks, and other public repositories of hacker community discussions are continuously monitored, collected and aggregated in order to locate mentions of business names and websites. The Hacker Chatter score is an informational indicator ranking that is ranked based on the quantity of indicators that appear within the collection sensors.



No issues found.



INFORMATION LEAK

ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

This Information Leak module makes use of chatter monitoring and deep web monitoring capabilities to identify compromised credentials being circulated by hackers. These come in the form of bulk data breaches announced publicly as well as smaller breaches, and smaller exchanges between hackers.



There are no High Risk Issues to detect for Information Leak

MEDIUM SEVERITY

There are no Medium Risk Issues to detect for Information Leak

LOW SEVERITY

Sensitive Application Information Exposed (GitHub)

Sensitive Application Information Exposed (Google)

Credentials at Risk

✓ POSITIVE SIGNALS

There are no Positive Risk Issues to detect for Information Leak

1 INFORMATIONAL

There are no Info Risk Issues to detect for Information Leak

No issues found.



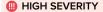
SOCIAL ENGINEERING

ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found

ABOUT THIS FACTOR

The SecurityScorecard Social Engineering Module is used to determine the potential susceptibility of an organization to a targeted social engineering attack. The Social Engineering module ingests data from social networks and public data breaches, and blends proprietary analysis methods. The Social Engineering Score is an informational indicator calculated based on the quantity of indicators that appear in SecurityScorecard collection sensors.



There are no High Risk Issues to detect for Social Engineering

MEDIUM SEVERITY

There are no Medium Risk Issues to detect for Social Engineering

1 LOW SEVERITY

Employee Satisfaction

Corporate Email Used on Marketing Sites

Short-Term Lending Site

✓ POSITIVE SIGNALS

There are no Positive Risk Issues to detect for Social Engineering

1 INFORMATIONAL

Leaked Company Emails Open to Spear-Phishing

62

No content (including ratings, data, reports, software or other application or output therefrom) or any part thereof (collectively, Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system without the prior written permission of SecurityScorecard, Inc. (SSC) The Content shall not be used for any unlawful or unauthorized purposes.

SSC and any third-parties, and their directors, officers, shareholders, employees, customers and agents (collectively SSC Parties) do not guarantee or warrant the accuracy, completeness, timeliness or availability of the Content. SSC Parties are not responsible for any errors or omissions (negligent or otherwise), regardless of the cause, or for the results obtained from the use of the Content. The Content is provided on an "as is" basis. SSC PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS,(3) FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall SSC Parties be liable to any party for any direct, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

USERS OF THE CONTENT MUST USE ALL REASONABLE ENDEAVORS TO MITIGATE ANY LOSS OR DAMAGE WHATSOEVER (AND HOWSOEVER ARISING) AND NOTHING HEREIN SHALL BE DEEMED TO RELIEVE OR ABROGATE USERS OF ANY SUCH DUTY TO MITIGATE ANY LOSS OR DAMAGE.

IN ANY EVENT, TO THE EXTENT PERMITTED BY LAW, THE AGGREGATE LIABILITY OF THE SSC PARTIES FOR ANY REASON WHATSOEVER RELATED TO ACCESS TO OR USE OF CONTENT SHALL NOT EXCEED THE GREATER OF (A) THE TOTAL AMOUNT PAID TO SSC BY THE USER FOR SERVICES PROVIDED DURING THE 12 MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO LIABILITY, AND (B) U.S. \$100.

Security-related analyses, including ratings and statements in the Content, are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SSC's opinions, analyses and ratings should not be relied on as a substitute for the skill, judgment and experience of the user and its management, employees, advisors and clients when making business decisions. SSC assumes no obligation to update the Content following publication in any form or format. While SSC has obtained information from sources it believes to be reliable, SSC does not perform an audit and undertakes no duty of due diligence or independent verification of any information it receives. Users expressly agree that (a) the security ratings and other security opinions provided via the Content do not reflect, identify or detect every vulnerability or security issue or address any other risk; (b) the security ratings and other opinions provided do not take into account users' particular objectives, situations or needs; (c) each rating or other opinion will be weighed, if at all, solely as one factor in any decision made by or on behalf of any user; and (d) users will accordingly, with due care, make their own study and evaluation of the risks of doing business with any entity. If a user identifies any in the Content, we invite you to share that information with us by emailing us at support@securityscorecard.io. © 2017 SecurityScorecard, Inc. All rights reserved.